ACADEMIA ROMÂNA

SECȚIA DE ȘTIINȚA ȘI TEHNOLOGIA INFORMAȚIEI

Institutul de Cercetări pentru Inteligență Artificială "Mihai Drăgănescu"

Institutul de Cercetări pentru Inteligenţă Artificială "Mihai Drăgănescu" --- **Sectorul Financiar Contabil, Administrativ şi Personal, Departamentele de cercetare**	**PROCEDURA OPERAȚIONALĂ privind administrarea şi asigurarea securităţii echipamentelor şi sistemelor ICIA** **Cod: P.O. 42**	**Ediția: 1** **Nr.de ex.: 1** **Revizia: -** **Nr.de ex. : 1** **Pag. 1 din 22** **Exemplar nr.: 1**

1. Lista responsabililor cu elaborarea, verificarea şi aprobarea ediţiei sau, după caz, a reviziei în cadrul ediţiei procedurii operaţionale

	Elemente privind responsabilii /operatiunea	Numele şi prenumele	Funcţia	Data	Semnătura
1.1.	Elaborat	Marius Ionut Sucu	Ing. De Sistem	02.11.2020	
1.2.	Verificat	Vasile Pais	CS III	26.11.2020	
1.3.	Aprobat	Ioan Dan Tufis	Presedinte CSCIM	02.12.2020	
1.4.	Aprobat	Ioan Dan Tufis	Director ICIA	02.12.2020	

1. Situatia editiilor si a reviziilor in cadrul editiilor procedurii operationale

	Editia/Revizia in cadrul editiei	Componenta revizuita	Modalitatea reviziei	Data de la care se aplica
2.1.	**Editia 1**	**x**	**x**	**2.12.2020**
2.2.	**Revizia 1**			
2.3.	**Revizia 2**			

2. Lista cuprinzand persoanele la care se difuzeaza editia sau, dupa caz, revizia din cadrul editiei procedurii operationale

	Scopul difuzarii	Compart.	Functia	Nume si prenume	Data primirii	Semnatura
3.1.	Elaborare	SFCAP	Ing. Sist	Marius Sucu	02.11.2020	
3.2.	Verificare	Cercetare	CS III	Vasile Pais	26.11.2020	
3.3.	Aprobare	CSCIM	Presedinte CSCIM	Ioan Dan Tufis	02.12.2020	
3.4.	Aprobare	Director	Director	Ioan Dan Tufis	02.12.2020	

	Scopul difuzarii	Compart.	Functia	Nume si prenume	Data primirii	Semnatura
3.5.	Informare	Conducere	Director, Director Adjunct	Ioan Dan Tufis, Angela Ionita	02.12.2020	
3.6.	Informare	Departamente Cercetare, SFCAP	Toti angajatii	Toti angajatii	02.12.2020	Publicare pe site-ul ICIA
3.7.	Aplicare	Departamente Cercetare, SFCAP	Toti angajatii	Toti angajatii	02.12.2020	
3.8.	Arhivare	SFCAP	Responsabil arhivare	Contabil Sef	02.12.2020	
3.9.	Alte scopuri	-	-	-	-	-

3. Scopul procedurii

Această procedură are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii sistemelor informatice din cadrul Institutului de Inteligenta Artificiala "Mihai Draganescu".

Confidenţialitatea se referă la protejarea datelor împotriva accesului neautorizat.

Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la Sistemele Informatice şi de Comunicaţii.

Integritatea se referă la măsurile şi procedurile utilizate împotriva modificărilor sau distrugerii neautorizate.

Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor sistemelor informatice şi de comunicaţii. Sistemele informatice utilizate au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare.

De asemenea, această procedură are ca scop stabilirea cadrului necesar pentru elaborarea procedurilor legate de gestionarea şi utilizarea sistemelor informatice şi de comunicaţii.

5. Domeniul de aplicare

5.1. Precizarea (definirea) activitatii la care se refera procedura operationala

Procedura se refera la activitatea de administrare a sistemului informatic executata de catre Inginerul de sistem, stabilind totodata regulile, normele si masurile de siguranta si protectie a datelor si informatiilor din sistemul informatic.

5.2.Delimitarea explicita a activitatii procedurate in cadrul portofoliului de activitati desfasurate de ICIA

Intreaga activitate a departamentelor de cercetare si a SFCAP se desfasoara informatizat astfel incat administrarea si securizarea echipamentelor si sistemulului trebuie procedurata distinct.

5.3. Principalele activitati de care depinde si/sau care depind de activitatea procedurata

De activitatea procedurată depind toate celelalte activitati din cadrul ICIA, din cauza rolului pe care aceasta activitate il are in cadrul derularii corecte si la timp a tuturor proceselor.

6. Documente de referinţă

- Conventia Consiliului Europei privind criminalitatea informatica, adoptata la Budapesta la 23 noiembrie 2001
- Legea nr 87/2017 pentru modificarea Legii nr. 161/2003 privind unele masuri pentru asigurarea transparentei in exercitarea demnitatii publice, a functiilor publice si in

mediul de afaceri , prevenirea si sanctionarea coruptiei, Publicat in Monitorul Oficial, Partea I nr. 313 din 02/05/2017.
- Legea nr 128/2017 pentru modificarea si completarea Legii nr. 161/2003 privind unele masuri pentru asigurarea transparentei si exercitatea demnitatii publice, a functiilor publice in mediul de afaceri, prevenirea si sanctionarea coruptiei.
- Legea nr. 235/2015 pentru modificarea si completarea Legii nr. 506/2004 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice.
- Legea nr. 187/2012 pentru punerea in aplicare a Legii nr 286/2009 privind Codul penal, Publicat in Monitorul Oficial, Partea I nr. 757 din 12/11/2012
- Legea nr. 272/2006 pentru completarea art. 7 din Legea nr 506/2001 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice, publicat in Monitorul Oficial, Partea I nr. 576 din 04/07/2006.
- Legea nr. 64/2004 pentru ratificarea Conventiei Consiliului Europei privind criminalitatea informatica, adoptata la Budapesta la 23 noiembrie 2001, Publicat in Monitorul Oficial, Partea I nr. 343 din 20/04/2004.
- Legea nr 506/2004 privind prelucrarea datelor cu caracter personal si protectia vietii private in sectorul comunicatiilor electronice, Publicat in Monitorul Oficial, Partea I nr. 1101 din 25/11/2004.
- Legea nr 161/2003 privind unele masuri pentru asigurarea transparentei in exercitarea demnitatilor publice, a functiilor publice si in mediul de afaceri, prevenirea si sanctionarea coruptiei, Publicat in Monitorul Oficial, Partea I nr 279 din 21/04/2003
- Legea nr 455/2001 privind semnatura electronica, Publicat in Monitorul Oficial, Partea I nr. 429 din 31/07/2001
- Ordin nr 184/2004 pentru aprobarea Documentului de politica si strategie privind implementarea serviciului universal in sectorul comunicatiilor electronice, publicat in Monitorul Oficial, Partea I nr 508 din 07/06/2004
- Ordin nr 252/2003 pentru aprobarea Normelor metodologice privind instruirea si specializarea in domeniul informaticii a functionarilor publici, Publicat in Monitorul Oficial, Partea I nr 432 din 19/06/2003

- Ordin nr 52/2002 privind aprobarea cerintelor minime de Securitate a prelucrarilor de date cu caracter personal, publicat in Monitorul Oficial, Partea I nr 383. din 05/06/2002
- H.G. nr 1007/2001 pentru aprobarea Strategiei Guvernului privind Informatizarea administratiei publice, Publicat in Monitorul Oficial, Partea I nr 705 din 06/11/2001
- O.U.G. nr 34/2006 privind atribuirea contractelor de achizitie publica, a contractelor de concesiune de lucrari publice si a contractelor de concesiune de servicii.
- Ordinul nr 201/2016 pentru aprobarea Normelor metodologice privind coordonarea indrumarea metdologica si supravegherea stadiului implementarii si dezvoltarii sistemului de control intern managerial la entitatile publice a aparut in Monitorul Oficial, din 12.04.2016.
- Ordin nr 600/2018 privind aprobarea Codului controlului intern al entitatilor publice Publicat in Monitorul Oficial, Partea I nr. 387 din 07.05.2018
- Regulamentul de organizare si functionare a ICIA aprobate de Prezidiul Academiei Romane in 18 noiembrie 2020

7. Abrevieri

ICIA - Institutul de Cercetari pentru Inteligenta Artificiala "Mihai Draganescu"
SFCAP - Sectorul Financiar Contabil, Administrativ si Personal
CSCIM - Comisia pentru implementarea Standardelor de Control Intern Managerial

8. Descrierea procedurii

8.1. Politica de IT&C a ICIA

Resursele informatice şi de comunicaţii ale ICIA sunt bunuri strategice ale Academiei Romane şi sunt parte integrantă a acesteia. ICIA a investit substanţial in resursele sale pentru a putea crea acest sistem şi de aceea trebuie administrat ca atare. Compromiterea securităţii acestor resurse poate afecta capacitatea Intitutului de Inteligenta Artificiala de a utiliza si oferi servicii informatice şi de comunicaţii in domeniul sau activitate şi poate conduce la fraude, incidente legate de confidenţialitatea datelor cu caracter personal, la distrugerea datelor, la violarea

clauzelor contractuale, divulgarea secretelor, la afectarea credibilităţii ICIA în faţa partenerilor săi.

Această politică este stabilită astfel încât:

-să fie în conformitate cu regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice şi de comunicaţii;
-să stabilească practici prudente şi acceptabile privind utilizarea resurselor informatice şi de comunicaţii ale ICIA;
-să instruiască utilizatorii care au dreptul de folosire a acestor resurse privind responsabilităţile asociate utilizării acestora;
-să protejeze investiţia;
-să protejeze informaţiile conţinute în aceste sisteme;
-să reducă riscurile legale;
-să protejeze renumele Intitutului de Inteligenta Artificiala.

Utilizatorul se defineste ca fiind orice angajat al ICIA care are acces la resursele informatice ale ICIA dar si orice lt utilizator extern ICIA care acceseaza serviciile oferite de ICIA in domeniul sau de activitate.

8.2. Confidentialitate

În scopul administrării Resurselor Informatice şi de Comunicaţii ale ICIA şi pentru asigurarea securităţii acestora, personalul poate revizui sau utiliza orice informaţie stocată pe/sau transportată prin sistemele Resurselor Informatice şi de Comunicaţii în conformitate cu legile în vigoare.

Utilizatorii vor avea grijă să nu încalce drepturile de confidenţialitate ale altor persoane atunci când utilizează echipamentele (de exemplu, când fac înregistrări audio-video la locul de muncă s.a.).

Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al echipamentelor din cadrul ICIA, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament.

Utilizatorul trebuie să se asigure prin mijloace legale sau tehnice că informaţiile aparţinând sau aflate în custodia si sub controlul ICIA în orice moment.

Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele ICIA pentru care nu au autorizaţie sau consimţământ explicit.

Nici un utilizator al resurselor informatice şi de comunicaţii ale ICIA nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemelor ce compun resursele informatice şi de comunicaţii. Această regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu ICIA.

Stocarea de informaţii în interes de serviciu pe dispozitive aflate în afara controlului ICIA, inclusiv pe dispozitive administrate de terţi cu care ICIA nu are un acord contractual, este interzisă. Se interzice în mod expres utilizarea în interes de serviciu a unui cont de e-mail care nu este furnizat de ICIA.

Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicaţii ale terţilor nu poate fi garantată. Utilizatorii sunt obligaţi să se asigure că toate informaţiile confidenţiale ale ICIA se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

8.3. Administrarea conturilor

Pentru toate conturile create trebuie să existe asociată o cerere ap catre inginerul de Sistem si Directorul ICIA. Toate conturile de acces se vor crea în formatul standard cont utilizator prenume.nume.

Prin contractul de muncă şi/sau alte documente toţi utilizatorii acceptă prevederile regulamentelor privind securitatea sistemului informatic şi de comunicaţie.

Toţi utilizatorii sunt obligaţi să păstreze confidenţialitatea informaţiilor privind contul de acces.

Toate conturile trebuie să se poată identifica în mod unic, utilizând numele de cont asociat.

Toate parolele pentru conturi trebuie să fie create şi folosite în conformitate cu politica privind parolele de acces.

8.4. Acordare si retragerea accesului la date, sisteme informatice si site-uri web

Acordarea accesului pentru angajaţi se va face de către Inginerul de Sistem al ICIA în urma transmiterii de către Consilierul Juridic cu atributii de referent resurse umane din ICIA a unei instiintari care va conţine detalii legate de utilizator şi drepturile acestuia. Instiintarea se va retrimite în cazul modificării numelui utilizatorului, a drepturilor utilizatorului ca urmare a schimbării postului de lucru sau în cazul încetării contractului de muncă.

Acordarea accesului pentru vizitatori se va face de către Inginerul de Sistem al ICIA în urma transmiterii de către Secretariat, a unei instiintari care va conţine detalii legate de vizitator şi drepturile acestuia.

Acordarea accesului pentru vizitatori, pentru furnizori sau alte categorii de utilizatori, se va face de către Inginerul de Sistem al ICIA în urma transmiterii de către persoanele interesate a unei cereri ce va conţine detalii legate de utilizator precum şi legate de durata activării contului de utilizator şi drepturile acestuia.

Accesul la sistemele informatice şi site-urile web utilizate ICIA se va face conform drepturilor de acces mentionate in Fisa de Sracini si Atributuni a angajatului.

8.5. Identificare si autentificare

Utilizatorul este responsabil pentru securitatea datelor, a informaţiilor de autentificare şi a sistemelor aflate sub controlul său.

Utilizatorul trebuie să păstreze credenţialele de acces (nume utilizator, parolă, token etc.) în siguranţă şi să nu le împărtăşească nici unei alte persoane, inclusiv colegi, membri ai familiei sau prieteni.

Asigurarea accesului altei persoane, fie în mod deliberat, fie prin incapacitatea de a păstra în siguranţă informaţiile de autentificare, reprezintă o încălcare a acestei politici.

Nu trebuie, sub nici o formă, să acceseze neautorizat fişierele, calculatoarele sau alte dispozitive din reţeaua ICIA. Acesta este considerat caz de fraudă majoră. La părăsirea calculatorului trebuie ca utilizatorul să iasă din reţea (log off).

De asemenea sunt interzise:

-încercarea utilizatorilor de a vizualiza şi deduce parolele altora în timpul introducerii acestora,

-transmiterea de parole în clar prin intermediul sistemelor de comunicaţii (e-mail, mesagerie instant, SMS etc.).

În situaţii justificate este permisă utilizarea de catre Inginerul de Sistem sau sub supravegherea lui a unor aplicaţii autorizate de management al parolelor. Altfel folosirea acestor aplicaţii pentru a stoca parole de domeniu, parole administrative sau parole de acces la aplicaţii sau servicii critice este interzisă.

8.6. Acces administrativ

Utilizatorii trebuie să faca dovada cunoasterii şi să accepte toate regulamentele privind securitatea sistemului informatic înainte de a li se permite accesul la un cont.

Cei care utilizează conturi de acces cu drepturi administrative sau speciale trebuie să folosească tipul de privilegiu cel mai potrivit activităţii pe care o desfăşoară.

Accesul administrativ trebuie să se conformeze politicii privind managementul parolelor

Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al Directorului ICIA şi trebuie să fie schimbată atunci când persoana care utilizează acest cont îşi schimbă locul de muncă în ICIA, sau în cazul unei modificări a listei de personal care furnizează servicii din partea terţilor având contracte cu ICIA.

Unele conturi sunt necesare pentru dezvoltare sau instalare de software sau alte operaţiuni definite. Acestea trebuie să îndeplinească următoarele condiţii:

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

8.7. Accesul la reteaua de comunicatii

Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către Inginerul de Sistem al ICIA.

Conectarea sistemelor de calcul care nu sunt proprietatea ICIA se face numai cu aprobarea în scris a Directorului ICIA.

Accesul de la distanţă la reţeaua ICIA se va realiza numai prin echipamente aprobate de catrfe Inginerul de Sistem al ICIA, folosind protocoale aprobate de către Inginerul de Sistem al ICIA şi conducerea ICIA.

Utilizatorii din interiorul reţelei de comunicaţie a ICIA nu se pot conecta la altă reţea.

Utilizatorii nu trebuie să extindă sau să retransmită serviciile de reţea în nici un fel (pe nici o cale). Nu este permisă instalarea de conexiuni de reţea neautorizate indiferent de motiv.

Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea Inginerului de Sistem al ICIA.

Sistemele computerizate din afara ICIA care necesită conectare la reţea trebuie să se conformeze standardelor reţelei interne ale ICIA.

Utilizatorii nu au dreptul să descarce, să instaleze sau să ruleze programe de securitate care pot dezvălui slăbiciuni în securitatea sistemului. De exemplu, utilizatorii ICIA nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua ICIA.

Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.

De Serviciul de administrare a numelor şi adreselor IP se ocupa exclusiv Inginerul de Sistem al ICIA. Serviciile de interconectare a reţelei ICIA cu alte reţele sunt realizate exclusiv de către Inginerul de Sistem.

Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Inginerului de sistem. Tipul şi modelul plăcilor de reţea şi al tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către Inginerul de Sistem al ICIA.

8.8. Configurarea sistemelor informatice pentru accesul la reteaua de comunicatii

Infrastructura de comunicaţii şi reţeaua de comunicaţii digitale a ICIA este administrată de către Inginerul de Sistem, care este responsabil cu întreţinerea şi dezvoltarea acesteia.

Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare, toate componentele acesteia sunt instalate de către Inginerul de Sistem sau de către un furnizor avizat explicit de către Inginerul de Sistem.

Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor Inginerului de Sistem.

Modificarea configuraţiei oricărui dispozitiv activ conectat la reţeaua de comunicaţii se face numai cu aprobarea Inginerul de Sistem.

Infrastructura de comunicaţii de date a ICIA suportă un set definit de protocoale de reţea (TCP/IP). Orice utilizare a altui set de protocoale trebuie să fie aprobată în scris de către Inginerul de Sistem.

Adresele de reţea sunt alocate dinamic sau static numai de către Inginerul de Sistem.

Toate conectările în reţeaua de comunicaţii a ICIA reprezintă sarcină a Inginerului de Sistem

Toate conectările dintre reţeaua de comunicaţii a ICIA şi alte reţele de comunicaţii, publice sau private, sunt responsabilitatea exclusivă a Inginerului de Sistem.

Echipamentele de protecţie a reţelei de comunicaţie a ICIA (firewall) se vor instala de către Inginerul de Sistem.

Utilizatorii nu au dreptul să extindă sau să retransmită în nici un fel serviciile reţelei (este interzisă instalarea unui modem, router, switch, hub sau punct de acces la reţeaua ICIA) fără aprobare din partea Inginerului de Sistem.

Utilizatorilor li se interzice instalarea de dispozitive hardware de reţea sau de programe care furnizează servicii de reţea fără aprobarea Inginerul de Sistem.

Utilizatorilor nu le este permis accesul la dispozitivele hardware ale reţelei.

8.9. Utilizarea echipamentelor

Utilizatorul este responsabil de păstrarea în siguranţă şi folosirea corectă în scopurile destinate şi autorizate a echipamentelor care i-au fost puse la dispoziţie de ICIA. Acestea includ staţii de lucru fixe şi mobile, imprimante, telefoane mobile şi fixe şi alte mijloace de procesare a informaţiilor, inclusiv software-ul asociat.

Toate staţiile de lucru trebuie să fie asigurate împotriva accesului neautorizat atunci când sunt lăsate nesupravegheate. Aceasta se poate face prin blocarea calculatorului, log off sau cu un screensaver protejat cu parolă, cu funcţia de activare automată setată la 5 minute sau mai puţin. La sfârşitul programului de lucru acestea, precum şi orice aparatură electrică şi electronică, trebuie să fie oprite.

De asemenea: CD-urile, DVD-urile, alte medii de stocare nu trebuiesc lăsate la vedere atunci când nu sunt folosite.

Daca ele conţin date de maximă confidenţialitate, trebuie să fie ţinute sub cheie. CD-urile, DVD-urile, mediile de stocare mobile trebuie păstrate departe de acţiunile mediului înconjurător cum ar fi: surse de căldura, lumina directă a soarelui şi câmpuri magnetice.

Următoarele acţiuni sunt strict interzise utilizatorilor:
-modificarea sau eliminarea măsurilor de securitate, inclusiv, dar fără a se limita la: dezinstalarea sau dezactivarea antivirusului ori modificarea setărilor de actualizare ale acestuia (actualizarea automată trebuie să fie activă), dezactivarea sau modificarea setărilor firewall- ului,
-instalarea de software neautorizat sau pentru care nu există licenţă valabilă la zi,
-scoaterea echipamentului în afara locaţiei fără autorizare prealabilă,
-introducerea şi utilizarea de produse care pun în pericol securitatea informaţiilor (dispositive sau software de ascultare, conectare, înregistrare sau copiere neautorizată) sau a personalului (arme de orice fel, produse toxice sau explozive etc.),
-eliminarea nesigură a mediilor de stocare sau a echipamentelor care au în componenţă medii de stocare.

8.10. Securitatea echipamentelor si resurselor in afara ICIA

Folosirea echipamentelor în afara locaţiei ICIA creşte riscurile de securitate ale acestora, echipamentele fiind în special vulnerabile la daune fizice, pierdere şi furt. În acest caz, se vor aplica următoarele măsuri de securitate:

- În momentul părăsirii ICIA, echipamentul poate fi utilizat pentru resursele online (ex. e- mail) şi va exista acces la informaţiile statice;
- Update-urile aplicaţiilor (de exemplu: sistem de operare, antivirus, Suita Office etc.) se vor face doar la revenirea cu echipamentul în reţeaua ICIA. Utilizatorul are obligaţia ca la un interval de maximum 2 săptămâni să introducă echipamentul în reţeaua internă a ICIA pentru actualizări ;
- Accesul la aplicaţiile de pe serverele ICIA (ex. Korap) se va face prin VPN cu aprobarea şefului direct, aprobarea pentru utilizarea VPN-ului fiind comunicată Inginerului de sistem;
- Documentele personale (valabil pentru toate echipamentele) se vor ţine într-un folder "Personal".

- Furtul sau pierderea unui echipament scos în afara ICIA vor fi raportate imediat şefului ierarhic şi Inginerului de sistem.

8.11. Utilizarea echipamentelor proprietate personala

ICIA poate permite angajaţilor sau persoanelor terţe să folosească echipamente proprietate personală (EPP) pentru îndeplinirea sarcinilor de serviciu.

Următoarele echipamente proprietate personală sunt permise:

-dispozitive de tip smartphone având sisteme de operare: iOS, Android, Blackberry sau Windows;
-tablete având sisteme de operare: iOS, Android, Windows;
laptop-uri;
-dispozitive de stocare portabile: stick-uri de memorie USB, carduri de memorie, hard-disk-uri portabile etc.

Utilizarea echipamentelor proprietate personală este asociată cu o serie de riscuri de securitate a informaţiilor, cum ar fi:

- pierderea, dezvăluirea sau alterarea informaţiilor ICIA stocate pe EPP;
- incidente care implică ameninţări la adresa infrastructurii informatice a ICIA sau compromiterea acestei infrastructuri (de exemplu: viruşi, malware, hacking);
- nerespectarea legilor, reglementărilor şi obligaţiilor contractuale (de exemplu, protecţia datelor cu caracter personal, legislaţia anti-piraterie etc.);
- nerespectarea drepturilor de proprietate intelectuală pentru informaţiile ICIA create, stocate, procesate sau transmise pe EPP.

Angajaţii care folosesc EPP pentru îndeplinirea sarcinilor de serviciu trebuie să fie autorizaţi în mod explicit să facă acest lucru. Autorizarea va fi dată de catre directorul ICIA ca răspuns la o solicitare în care este explicat motivul solicitării. Pentru autorizare, Inginerul de Sistem va putea cere informaţii despre EPP care va fi utilizat.

Utilizatorii trebuie să asigure aceleaşi măsuri de protecţie a informaţiilor ca şi cele aplicate pentru echipamentele ICIA şi nu trebuie să introducă riscuri inacceptabile (exemplu: malware) în reţeaua ICIA prin utilizarea de echipamente nesigure.

ICIA îşi rezervă dreptul de a refuza sau de a retrage autorizarea în cazul în care consideră că echipamentul nu este adecvat şi/sau nu este folosit în interesul institutului.

În timp ce utilizatorii au o aşteptare rezonabilă de intimitate asupra informaţiilor lor personale pe propriul echipament, dreptul ICIA de a controla propriile date şi de a gestiona EPP poate duce ocazional la accesul neintenţionat al personalului de asistenţă la informaţiile lor personale. Pentru a reduce posibilitatea unui astfel de acces, utilizatorii trebuie să păstreze datele lor personale separat de datele ICIA, în directoare/foldere separate, denumite în mod sugestiv.

8.12. Securizarea serverelor

Un server nu trebuie conectat la reţeaua ICIA până când nu se află într-o stare sigură, acreditată de către Inginerul de Sistem.

Securizarea serverelor trebuie să includă obligatoriu următoarele:

- Instalarea sistemului de operare dintr-o sursă aprobată;
- Aplicarea patch-urilor furnizate de producător;
- Înlăturarea programelor, a serviciilor sistem şi a driver-lor care nu sunt necesare;
- Setarea/activarea parametrilor de securitate, a protecţiilor pentru fişiere şi activarea jurnalelor de monitorizare;
- Dezactivarea sau schimbarea parolelor conturilor predefinite;
- Securizarea accesului fizic la aceste echipamente.

Inginerul de Sistem va monitoriza obligatoriu pentru serverele principale, procesul de instalare şi aplicarea regulată a patch-urilor de securitate.

8.13. Detectarea accesului neautorizat

Procesele de înregistrare şi verificare a activităţii sistemelor de operare, conturilor utilizator şi programelor trebuie să fie funcţionale pe toate sistemele active (host, server, echipamente de reţea).

Trebuie activate funcţiile de anunţare a persoanelor responsabile oferite de firewall-uri şi sistemele de control al accesului la reţea.

Trebuie activate funcţiile de înregistrare a evenimentelor pe dispozitivele firewall şi pe toate sistemele de control al accesului.

Înregistrările de verificare ale dispozitivelor de control al accesului trebuie monitorizate/revizuite (examinate) de către Inginerul de Sistem.

Verificările privind integritatea fiecărui sistem trebuie să se facă periodic. Această activitate este obligatorie şi pentru dispozitivele de tip firewall sau dispozitive de control al accesului.

Înregistrările de verificare pentru serverele din reţeaua internă trebuie revizuite periodic. Se vor verifica periodic programele utilitare pentru detectarea tentativelor de acces neautorizat.

Toate rapoartele privind incidentele trebuie verificate în vederea detectării de indicii ce ar putea implica o activitate de acces neautorizat.

Toate indiciile suspecte sau confirmate de accesări sau încercări de accesare neautorizate trebuie raportate imediat către Inginerul de Sistem.

Utilizatorii sunt obligaţi să raporteze orice anomalii în performanţa sistemelor utilizate cât şi orice semne ale unor posibile infracţiuni la Inginerul de Sistem.

8.14. Modificari ale configuratiei sistemului

Orice modificare asupra unei componente a configuraţiei sistemului din cadrul Institutului de Inteligenta Artificiala, cum ar fi: sisteme de operare, componente hardware, echipamente şi componente de reţea, aplicaţii, este supusă prezentului regulament şi trebuie să urmeze procedurile în vigoare.

Toate modificările care afectează mediul de funcţionare a sistemelor componente ale sistemului informatic (de ex: aparate de aer condiţionat, instalaţii de apă, încălzire, instalaţii electrice şi alarme) trebuie să fie anunţate şi aprobate în scris de departamentul care administrează resursele afectate.

Toate propunerile de modernizare şi extindere a elementelor de infrastructură ale sistemului informatic vor fi documentate şi aprobate de către Inginerul de Sistem. Nu este permisă modificarea de către utilizatori a elementelor de infrastructură ale sistemului informatic.

Modificările şi modernizările sistemelor de calcul vor fi documentate de către utilizator şi aprobate de către Inginerul de Sistem si Directorul ICIA.

Modificările planificate trebuie anunţate cu cel puţin 48 ore înainte de a fi executate.

Cererile de modificare planificate pot fi respinse în următoarele cazuri: planificare inadecvată, planuri de refacere a serviciilor inadecvate, durata modificării poate afecta în

mod negativ o activitate importantă a ICIA sau resursele corespunzătoare necesare nu pot fi disponibile imediat.

Inginerul de Sistem va întocmi un raport pentru orice modificare, indiferent dacă a fost planificată sau neplanificată, sau dacă s-a realizat sau nu cu succes.

Inginerul de Sistem trebuie sa întreţină o bază de date care să cuprindă toate modificările. Aceasta trebuie să conţină cel puţin următoarele informaţii:
- data la care s-a făcut cererea pentru modificare şi data la care s-a făcut modificarea;
- informaţii de contact pentru utilizator;
- natura modificării;
- indicarea succesului sau nereuşitei modificări.

8.15. Site-uri web ale ICIA

Toate site-urilor web aparţinând ICIA trebuie să se supună regulilor stabilite la nivelul ICIA din punct de vedere al aspectului şi al securităţii.

Nu se vor publica pe site-urile web ale ICIA materiale cu caracter ofensiv sau de hărţuire.

8.16. Mijloace de comunicatie

Adresa de e-mail furnizată de ICIA şi mailbox-ul asociat acesteia, adresa IP şi, după caz, numărul de telefon fix, telefon mobil şi conexiunea de date mobile sunt resurse puse la dispoziţia utilizatorilor de ICIA pentru a fi folosite la îndeplinirea sarcinilor de serviciu. Utilizarea ocazională în scop personal a acestora este permisă numai dacă nu afectează într-o măsură perceptibilă consumul de resurse al ICIA şi nu introduce riscuri suplimentare pentru ICIA.

Următoarele acţiuni sunt strict interzise utilizatorilor:
-utilizarea necorespunzătoare a mijloacelor de comunicare, inclusiv, dar fără a se limita la: sprijinirea activităţilor ilegale, procurarea şi distribuirea de materiale sau mesaje cu caracter ofensator, rasist, obscen, discriminator sau în scop de hărţuire, defăimare sau ameninţare,

-procurarea şi distribuirea neautorizată de materiale protejate de drepturile de autor (imagini, muzică, filme, mărci şi logo-uri ale altor companii preluate din reviste, ziare, cărţi sau de pe Internet),
-transmiterea de materiale protejate prin legea dreptului de autor fără permisiunea expresă,
-utilizarea mijloacelor de comunicare pentru publicitate neautorizată, relaţii de afaceri care nu implică sau sunt contrare intereselor ICIA, campanii politice, utilizarea în scop distractiv sau orice alte scopuri care nu au legătură cu activitatea ICIA,
-trimiterea de spam sau bombe e-mail prin intermediul sistemului de e-mail, mesajelor text, mesageriei instant, mesageriei vocale sau altor forme de comunicare electronică utilizate,
-falsificarea, denaturarea, ascunderea, suprimarea sau înlocuirea unei identităţi de utilizator, pe orice mijloc de comunicare electronică, cu scopul de a induce în eroare destinatarul cu privire la identitatea expeditorului,
-postarea sau transmiterea de mesaje non-business identice sau similare către un număr mare de destinatari (news-group spam),
-transmiterea de informaţii confidenţiale sau secrete de serviciu altor destinatari decât cei autorizaţi să primească aceste informaţii,
-utilizarea adresei de e-mail sau a adresei IP pentru a se angaja în activităţi care încalcă politicile sau orientările ICIA; postarea pe grupuri publice de ştiri, forumuri sau reţele sociale folosind adresa de e-mail sau adresa IP ale ICIA, reprezintă compania în faţa publicului şi prin urmare trebuie efectuată cu discernământ pentru a evita reprezentarea greşită sau depăşirea autorităţii de a reprezenta poziţia ICIA.

Orice mesaj şi/sau informaţie trimisă prin intermediul reţelelor publice pot fi identificate şi atribuite Institutului de Inteligenta Artificiala. Din acest motiv, postarea pe forumuri sau alte site-uri de informaţii care implică numele sau adrese de e-mail ale ICIA se va face fără furnizarea de informaţii confidenţiale sau care pot afecta reputaţia ICIA. Părerile personale exprimate pe astfel de site-uri sau forumuri vor fi însoţite de nota: "Părerile exprimate sunt personale şi nu reprezintă poziţia oficială a ICIA.

8.17. Utilizarea resurselor informatice in scop personal

Mijloacele de procesare a informaţiei puse la dispoziţie de ICIA sunt destinate în primul rând îndeplinirii sarcinilor de serviciu.

Utilizarea limitată în scopuri personale, ocazională sau accidentală, a mijloacelor de procesare a informaţiei este de înţeles şi acceptabilă, cu condiţia ca ea să se facă într-o manieră care să nu afecteze negativ utilizarea acestora pentru scopul principal.

Utilizatorii trebuie să demonstreze simţ de responsabilitate şi să nu abuzeze de acest drept.

Stocarea e-mail-urilor, documentelor şi altor fişiere personale nu este încurajată. În cazul în care acestea sunt totuşi păstrate, vor fi stocate local şi nu pe serverele ICIA, în locaţii separate de cele care conţin informaţii ce aparţin ICIA. Toate mesajele şi fişierele personale aflate în sistemul informatic pot fi supuse verificării de conformitate cu Politica IT&C a ICIA

ICIA nu îşi asumă nici o responsabilitate cu privire la securitatea acestor informaţii, întreaga responsabilitate (inclusiv realizarea copiilor de siguranţă) revenind utilizatorului.

8.18. Detectarea virusilor

Toate echipamentele desine stătătoare sau conectate la reţeaua de comunicaţii a ICIA trebuie să utilizeze programe antivirus aprobate de către Inginerul de Sistem.

Programele antivirus nu trebuie dezactivate.

Configuraţia programului antivirus trebuie să nu fie modificată într-un mod care să reducă eficacitatea programului.

Frecvenţa actualizărilor automate a programului antivirus trebuie asigurată de către utilizator.

Orice server conectat la reţeaua ICIA trebuie să utilizeze un program antivirus aprobat în scopul detectării şi curăţirii viruşilor care pot infecta fişierele puse la dispoziţie.

Orice server sau gateway pentru e-mail trebuie să folosească un program antivirus pentru e-mail aprobat şi trebuie să respecte regulile de instalare şi utilizare a acestui program.

Orice virus care nu a putut fi înlăturat automat de către programul antivirus constituie un incident de securitate şi trebuie raportat imediat Inginerului de Sistem.

8.19. Returnarea resurselor la terminarea contractului

Utilizatorul va returna ICIA, la încetarea contractului de muncă sau de servicii, orice informaţii şi orice mijloace de procesare a informaţiilor puse la dispoziţia sa în scopul îndeplinirii atribuţiilor de serviciu sau obligaţiilor contractuale. Acestea includ şi nu se limitează la: credenţialele de acces la sisteme critice, primite sau modificate pe perioada contractului ş.a.m.d.

8.20. Exceptii

Excepţiile de la regulile definite în această procedură vor fi puse în aplicare numai după autorizarea prealabilă a Inginerul de Sistem, care va fi solicitată în scris şi va include obligatoriu motivul excepţiei. Toate excepţiile vor fi considerate evenimente de securitate, vor fi comunicate Inginerului de Sistem şi vor fi înregistrate de acesta în Registrul incidentelor de securitate, specificând data şi ora, descrierea, motivul şi modul de gestionare a riscurilor.

9. Responsabilitati

Conducerea ICIA are următoarele responsabilităţi:

- stabileste şi aprobă procedura privind administrarea si asigurarea securitatii echipamentelor si sistemelor ICIA, procedurile subsecvente precum şi obiectivele de securitate a informaţiilor;
- asigură disponibilitatea resurselor necesare pentru aplicarea procedurii privind administrarea si asigurarea securitatii echipamentelor si sistemelor ICIA;
- se preocupa de gestionarea eficienta a sistemelor informatice şi de comunicaţii ale ICIA.

Conducerea Institutului si Inginerul de sistem:

- se asigură că sistemele informatice şi de comunicaţii sunt gestionate eficient;
- îndrumă şi sprijină personalul să contribuie la eficacitatea sistemele informatice şi de comunicaţii.

Inginerul de sistem are următoarele responsabilităţi:

- propune modificări ale Politicii IT&C;
- elaborează şi propune pentru aprobare politici şi proceduri de gestionare şi de securitate a resurselor informatice şi de comunicaţii în conformitate cu procedura privind administrarea si asigurarea securitatii echipamentelor si sistemelor ICIA
- tratează incidentele de securitate în scopul minimizării efectului distructiv al acestora asupra resurselor informatice şi de comunicaţii;
- informează conducerea în caz de incidente, intervenţie şi rezolvarea incidentelor de securitate a informaţiilor;
- planifică, verifică soluţiile de securitate a informaţiilor: server antivirus, firewall, server de actualizări de securitate, acces securizat la camera tehnică, asigurare aer condiţionat, asigurare alimentare cu energie electrică/UPS;
- menţine înregistrări privind configuraţia, aplicaţiile şi serviciile instalate (fişa de server), pentru a se putea reface sistemul în caz de dezastru;
- inventariază periodic aplicaţiile şi serviciile instalate şi verifică dacă sunt autorizate;
- administrează sistemele IT şi aplică măsurile de securitate şi alte cerinţe ale programului de securitate a informaţiilor pentru sistemele informatice pentru care are atribuită responsabilitatea.

Directorul ICIA, care are in subordine directa Inginerul de Sistem, este responsabil pentru:

- implementarea de zi cu zi a procedurii privind administrarea si asigurarea securitatii echipamentelor si sistemelor ICIA şi a procedurilor aferente acesteia;
- asigurarea că măsurile de securitate tehnice, fizice şi procedurale adecvate sunt implementate în conformitate cu Politica IT&C şi sunt aplicate în mod corespunzător şi de către tot personalul, asigurarea resurselor şi efectuarea analizelor necesare pentru a se asigura că informaţiile şi activele sunt protejate în mod corespunzător în zona lor de responsabilitate, informarea persoanei desemnate cu

managementul incidentelor de securitate despre încălcările reale sau presupuse ale Politicii IT&C care afectează securitatea informaţiilor din zona lor de responsabilitate (incidentele de securitate a informaţiilor), identificarea şi clasificarea informaţiilor şi echipamentelor din zona lor de responsabilitate şi desemnarea deţinătorilor (responsabililor) pentru acestea;

- informarea Inginerului de sistem la schimbarea responsabililor de echipamente.

Cuprins