CONTRACT DE SERVICII Nr. 3528/26.04.2022

Preambul

În temeiul Legii nr. 98/2016, privind achiziţiile publice precum si a Hotararii nr. 395 din 2 iunie 2016, pentru aprobarea Normelor metodologice de aplicare a prevederilor referitoare la atribuirea contractului de achiziţie publică/acordului-cadru,

I. PARTILE CONTRACTANTE

1.1. CREART - CENTRUL DE CREAȚIE, ARTĂ ȘI TRADIȚIE AL MUNICIPIULUI BUCUREȘTI, cu sediul in Mun. Bucuresti, Str. Piata Alexandru Lahovari, Nr. 7, Sect. 1, Tel. 318.38.03/04, cod fiscal 4266901, cont nr. RO57 TREZ 7012 1G33 5000 XXXX, deschis la Trezoreria Sector 1, reprezentat prin d-na Nicoleta Claudia Popa – Director, in calitate de **Achizitor,** pe de o parte,

Şi

1.2. **PERSOANA FIZICA AUTORIZATA,** cu sediul in
Nr. Ord in Reg. Com
deschis la Banca: ING Bank, in calitate de **Prestator,**

pe de alta parte.

DEFINITII

În prezentul contract următorii termeni vor fi interpretaţi astfel:

a) ***Contract*** - prezentul contract şi toate anexele sale;

b) ***achizitor şi prestator*** - părţile contractante, aşa cum sunt acestea numite în prezentul contract;

c) ***preţul contractului*** - preţul plătibil prestatorului de către achizitor, în baza contractului, pentru îndeplinirea integrală şi corespunzătoare a tuturor obligaţiilor asumate prin contract;

d) ***servicii*** - activităţi a căror prestare face obiect al contractului;

e) ***produse*** - echipamentele, maşinile, utilajele, piesele de schimb şi orice alte bunuri cuprinse în anexa/anexele la prezentul contract şi pe care prestatorul are obligaţia de a le furniza aferent serviciilor prestate conform contractului;

f) ***forţa majoră*** - reprezintă o împrejurare de origine externă, cu caracter extraordinar, absolut imprevizibilă şi inevitabilă, care se află în afara controlului oricărei părţi, care nu se datorează greşelii sau vinei acestora, şi care face imposibilă executarea şi, respectiv, îndeplinirea contractului; sunt considerate asemenea evenimente: războaie, revoluţii, incendii, inundaţii sau orice alte catastrofe naturale, restricţii apărute ca urmare a unei carantine, embargou, enumerarea nefiind exhaustivă, ci enunţiativă. Nu este considerat forţă majoră un eveniment asemenea celor de mai sus care, fără a crea o imposibilitate de executare, face extrem de costisitoare executarea obligaţiilor uneia din părţi;

g) zi - zi calendaristică; ***an*** - 365 de zile.

II. OBIECTUL CONTRACTULUI

2.1. Obiectul prezentului contract consta in intretinerea de catre Prestator in folosul Achizitorului a infrastructurii IT, respectiv executarea serviciilor de asistenta tehnica informatica (CPV–72000000-5) pentru echipamentele ce apartin acestuia din urma precum si pentru orice echipamente tehnice informatice achizitionate pe durata contractului, astfel cum sunt enumerate in anexa 1 la contract, conform anuntului de atribuire in SEAP, ofertei financiara transmisa de Prestator si inregistrata de Achizitor cu nr. 3430/19.04.2022, precum si a caietului de sarcini nr. 2988/05.04.2022.

III. VALOAREA CONTRACTULUI SI MODALITATI DE PLATA

3.1. Pretul contractului pentru intretinerea infrastructurii IT ce va fi achitat de catre Achizitor, Prestatorului (indiferent de numarul echipamentelor ce apartin Achizitorului), incepand cu data de 01.05.2022 si pana la data de 31.12.2022, este de 76.000 lei, fara TVA, respectiv suma de 9.500 lei fara TVA/luna, conform anuntului de atribuire in SEAP, ofertei financiara transmisa de Prestator si inregistrata de Achizitor cu nr. 3430/19.04.2022, precum si a caietului de sarcini nr. 2988/05.04.2022.

3.2. Factura aferenta serviciilor ce se constituie obiect la prezentului act va fi achitata de catre Achizitor in termen de maxim 30 de zile de la finalizarea acestora, dupa semnarea procesului verbal de receptie aferent, de catre ambele parti.
3.3. In cazul in care Achizitorul nu achita facturile aferente in termen de maxim 30 de zile de la data prestarii serviciilor de catre Prestator din motive neimputabile cauzate de nevirarea fondurilor necesare de la ordonatorul principal de credite, Prestatorul nu are dreptul de a pretinde plata de daune-interese.Achizitorul va achita contravaloarea facturilor neachitate din motive neimputabile în termen de maxim 15 zile de la data virării fondurilor cu această destinație.

IV. DURATA CONTRACTULUI

4.1. Prezentul contract este valabil incepand cu data semnarii sale si pana la indeplinirea tuturor obligatiilor contractuale ce decurg din executarea sa de catre parti.
4.2. Prestatorul va executa in folosul Achizitorului serviciile ce fac obiectul prezentului contract, incepand cu data de 01.05.2022 si pana la data de 31.12.2022.
4.3. Contractul poate fi prelungit la incetarea acestuia, de comun acord de catre parti, prin act aditional, pe o durata de patru luni, conform prevederilor legale

V. OBLIGATIILE PARTILOR CONTRACTANTE

5.1. Achizitorul in cadrul prezentului contract are urmatoarele obligatii :
a sa-l remunereze pe Prestator pentru serviciile prestate, stabilite de comun acord cu Achizitorul ;
b. sa creeze Prestatorului conditii corespunzatoare de lucru, cu respectarea normelor de protectia muncii;
c. să furnizeze Prestatorului toate informatiile necesare in vederea realizarii serviciilor ce se constituie obiect al prezentului contract ;
d. să achite la termenul stabilit prețul serviciilor prestate, conform clauzei III, sus mentionata ;

5.2. Prestatorul, in cadrul prezentului contract, se obliga :
a. sa execute serviciile de asistenta tehnica informatica sus mentionate pentru echipamentele ce apartin Achizitorului precum si pentru orice echipamente tehnice achizitionate pe durata contractului, incepand cu data de 01.05.2022 si pana cel tarziu in data de 31.12.2022, conform anuntului de atribuire in SEAP, oferta financiara transmisa de Prestator si inregistrata de Achizitor cu nr. 3430/19.04.2022, precum si a caietului de sarcini nr. 2988/05.04.2022.
Prestatorul va fi responsabil cu administrarea și întreținerea serverelor prezentate în anexa 1 la prezentul contract, respectiv :

- să asigure buna funcționare a echipamentelor prin revizii periodice și diagnosticare și/sau reparații prin înlocuirea componentelor defecte și/sau uzate precum și repunerea în funcțiune a echipamentelor indicate în prezentul Caiet de Sarcini.Toate componentele necesare vor fi achizitionate de catre Achizitor .

Prestatorul se obliga sa asigure :
- Asistență hardware pentru selectarea soluțiilor de securizare a rețelelor, precum și pentru menținerea performanțelor sistemelor.
- Servicii de informare a personalului cu ultimele cunoștințe despre produsele software utilizate în activitățile curente de întreținere.
- Instalarea ultimelor versiuni ale Service Pack-urilor produselor instalate și informarea periodică referitor la apariția acestora.
- Sprijin în achiziția de noi echipamente sau de upgrade pentru sistemele existente care coincid cu arhitecturile existente la sediul Achizitorului .
- Service pentru calculatoare:

i. Întreținere
- Teste de diagnosticare/funcționalitate (teste specifice pentru procesor, memorie, placă video, hard disk, placă de retea, etc);
- Verificare tensiuni sursă alimentare;
- Verificare funcționare ventilatoare;
- Verificare de viruși și devirusare;
- Actualizare sisteme de operare, aplicații, utilitare;
- Configurare regiștri;
- Mentenanță HDD (testare, defragmentare).

ii. Reparații
- Hardware:

o Înlocuire componente defecte.
- Software:
o Reconfigurare/reinstalare aplicații software (pachet Office, antivirus, utilitare, aplicații legislative, aplicații economice).
o Devirusare.
o Salvare și recuperare de date.
o Configurare conexiune rețea.
o Configurare client local de mail.
o Instalare/configurare aplicații semnatură digitală, și criptare.
- Service pentru echipamente de protecție (UPS):
i. Întreținere
- Desprăfuire internă a echipamentului utilizând instrumente specifice de aspirație sau de înlăturare a prafului.
- Teste de diagnosticare/funcționalitate.
- Verificare stare acumulatori.
ii. Reparații
- Hardware:
o Înlocuire componente defecte și/sau uzate.
o Înlocuire acumulatori.
- Software:
o Reconfigurare/reinstalare aplicații software.
- Service pentru echipamente active de retea:
i. Întreținere
- Teste de diagnosticare/funcționalitate.
ii. Reparații
- Hardware:
o Înlocuire componente defecte și/sau uzate.
o Up-grade echipamente.
o Montare, configurare echipamente rețea.
- Software:
o Reconfigurare/reinstalare firmware și/sau aplicații software.
- Service pentru echipamente pasive de rețea:
i. Întreținere
- Verificare a sistemului de răcire al dulapurilor de comunicații.
- Verificare stare trasee cablare structurată.
- Verificare stare prize de date.
- Verificare stare patch-cord-uri.
ii. Reparații
- Hardware:
o Înlocuire componente defecte și/sau uzate.
✓ Prestatorul va fi responsabil cu administrarea și întreținerea serverelor prezentate în ANEXA 1,
- Instalări/configurari sisteme de operare, softuri diverse;
- Administrare HyperV – hypervisor și mașini virtuale;
- Administrare mașini virtuale (linux, windows, linux personalizat – management firewall);
- Administrare sistem mesagerie electronică (email) pentru 70-100 utilizatori (creare/ștergere/modificare cont); monitorizare servicii;
- Administrare sistem antispam/antivirus cloud, creare/ștergere/modificare utilizatori, white/black lists, administrare carantină per utilizator și troubleshooting trafic mesagerie electronică.

6.2 STORAGE - NAS:
- Administrare soluție NAS – useri/grupuri de lucru stucturate logic;
- Administrare aplicații diverse NAS – Qsync, Backup, Cloud Link, File Station;
- Integrare servicii NAS in sistemul IT;
- Monitorizare servicii NAS, spațiu disc;

6.3 STAȚII DE LUCRU ȘI LAPTOPURI:
Prestatorul va fi responsabil cu administrarea și întreținerea stațiilor de lucru și a laptopurilor prezentate în ANEXA 1,
- Intervenția și înlocuirea sau repararea acestora în cel mai scurt timp, astfel încât să fie funcționale și software-ul instalat pe acestea, precum și toate perifericele legate la ele (monitoare, tastatură, mouse, imprimante, scanere, etc.) ;
- Instalări/configurări sisteme de operare, softuri diverse;
- Investigații defecte în vederea asigurării garanției (inclusiv asigurarea relației cu compania care asigură garanția – transport, etc);
- Instalări/configurări certificate digitale și diverse alte cerințe specifice de conectare ale unor servicii/produse specializate (SEAP, semnatură electronică, forexe, conexiuni bănci);
- Administrare soluție antivirus – consolă cloud. Instalare/configurare stații, administrare politici de securitare, monitorizare activă servicii și raportări pe activități cheie (update/virusare/etc);

6.4 PERIFERICE:
Prestatorul va fi responsabil cu instalarea și întreținerea perifericelor prezentate în ANEXA 1 (imprimante, scanere, etc.).

6.5 REȚEA:
Prestatorul va fi responsabil cu administrarea elementelor active, prezentate în ANEXA 1 și pasive de rețea, întreținerea, intervenția și înlocuirea acestora în cel mai scurt timp. Responsabilitatea achiziționării unor eventuale echipamente noi este sarcina Autorității contractante.
Prestatorul va fi responsabil cu asigurarea conexiunii permanente a tuturor calculatoarelor din cadrul creart la rețeaua internă.
Prestatorul va fi responsabil de setarea accesului utilizatorilor la diverse resurse ale rețelei interne și la Internet.

6.6 SOFTWARE:
Prestatorul va fi responsabil cu întreținerea/ instalarea/ reinstalarea/ configurarea/ updatarea corectă și eficientă a produselor software prezentate în ANEXA 1 (sisteme de operare, aplicații, utilitare de bază furnizate împreună cu acestea sau instalate ulterior).

6.7 FIREWALL:
Prestatorul va fi responsabil cu :
- Administrare soluție firewall NGTX - Gateway - Firewall, VPN, Advanced Networking and Clustering, Identity Awareness, Mobile Access, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, Content Awareness, SandBlast Threat Emulation, SandBlast Threat Extraction; Creare/modificare/implementare politici de Securitate; Monitorizare semnaturi noi IPS/AV și implementarea lor în funcție de necesități;
- Administrare soluție firewall NGTX – Management - Network Policy Management, Logging and Status, Monitoring, Smart Event SIEM;
- Troubleshooting și depanare trafic rețea, inclusiv deschidere tichete suport la producator și asigurarea relației cu producatorul pentru rezolvarea bug-urilor, diverselor probleme de configurare, situații de garanție;
- Upgrade la versiuni superioare (cu teste de staging în prealabil), inclusiv migrare soluție de la platforma cu deployment centralizat la platforma cu deployment distribuit (appliance & mediu virtual);
- Asigurare de personal certificat de către producător;

6.8 TIMPI DE INTERVENȚIE ȘI RĂSPUNS ȘI DISPONIBILITATE A SERVICIILOR:
Disponibilitatea serviciilor: 8 ore zilnic, 5 zile pe săptămână
Timp de răspuns: 30 minute
Timp de intervenție: 60 minute
Timp de rezolvare: 60 minute

b. sa execute serviciile prevazute in contract cu profesionalismul si promtitudinea cuvenite angajamentului asumat, in conformitate cu propunerea sa tehnica;

c. sa supravegheze prestarea serviciilor, sa asigure resursele umane, materiale, instalatiile, echipamentele si orice alte asemenea, fie de natura provizorie, fie definitiva, cerute prin contract, in masura in care necesitatea asigurarii acestora este prevazuta in contract sau se poate deduce in mod rezonabil din contract;

d. este pe deplin responsabil pentru executia serviciilor în conformitate conform prezentului act.Totodată, este răspunzător atât de siguranța tuturor operațiunilor și metodelor de prestare utilizate, cât și de calificarea personalului folosit pe toată durata contractului.

e. sa nu transfere total sau partial obligatiile asumate prin prezentul act, fara sa obtina in prealabil, acordul scris al Achizitorului .

VI. RASPUNDEREA CONTRACTUALA

6.1 În cazul în care din vina sa exclusivă, Prestatorul nu reuşeşte să-şi execute obligaţiile asumate prin contract, atunci Achizitorul are dreptul de a deduce din preţul contractului, ca penalităţi, o sumă echivalentă cu o cota de 0,01% pe zi din preţul contractului până la îndeplinirea efectivă a obligaţiilor.

6.2 În cazul în care Achizitorul nu îşi onorează oblugaţiile în termenul contractual convenit atunci acestuia îi revine obligaţia de a plăti, ca penalităţi, o sumă echivalentă cu o cotă procentuală de 0,01% din plata neefectuată pentru fiecare zi întârziere, până la îndeplinirea efectivă a obligaţiilor dar nu mai puţin decât dobânda legală penalizatoare calculată conform Legii nr. 72/2013 privind măsurile pentru combaterea întârzierii în executarea obligaţiilor de plată a unor sume de bani rezultând din contracte încheiate între profesionişti şi între aceştia şi autorităţi contractante

6.3 Nerespectarea obligaţiilor asumate prin prezentul contract de către una dintre părţi, în mod culpabil, dă dreptul părţii lezate de a considera contractul reziliat de drept şi de a pretinde plata de daune-interese.

6.4 a) Achizitorul îşi rezervă dreptul de a denunţa unilateral contractul de servicii, în cel mult 30 de zile de la apariţia unor circumstanţe care nu au putut fi prevăzute la data încheierii contractului şi care conduc la modificarea clauzelor contractuale în aşa măsură încât îndeplinirea acestuia ar fi contrară interesului public.

b) Achizitorul are dreptul de a denunţa unilateral prezentul contract şi în situaţia în care alocarea resurselor financiare a fost sistată.

VII. DOCUMENTELE CONTRACTULUI

7.1. Documentele contractului sunt:

a) oferta financiara nr. 3430/19.04.2022, atasata la prezentul act, transmisa Achizitorului in baza anuntului de atribuire in SEAP, Caietul de sarcini nr. 2988/05.04.2022 ;

b) Documente aferente procedurii de achizitie proprii initiate de Achizitor, inclusiv documentatia aferenta transmisa de Prestator .

c) Anexe la contract :

a) Anexa nr. 1- Prezentare echipamente tehnice informatice ce apartin Achizitorului .
b) Anexa nr. 2. Politica de prelucrare a datelor folosind echipamente mobile si lucrul la distanta ;
c) Anexa nr. 3- Politica de utilizare a resurselor informatice ;
d) Anexa nr. 4- Politica privind relatiile cu tertii ;
e) Anexa nr. 5- Politica privind parolarea ;
f) Anexa nr. 6 – Politica in domeniul transferului de informatii ;
g) Anexa nr. 7 - Procedura de management al incidentelor de securitate a informatiei ;
h) Anexa nr. 8- Politica de securitate privind sistemul resurselor informatice si de comunicatii .
i) Anexa nr. 9- Politica de stocare a datelor ce au caracter personal .

VIII. ÎNCETAREA CONTRACTULUI

8.1. Prezentul contract încetează de plin drept fără a fi necesară intervenţia vreunei instanţe judecătoreşti, în cazul când oricare dintre părţi:

a. nu-şi execută una dintre obligaţiile esenţiale enumerate la clauza V , din prezentul contract.

b. este declarată în incapacitate de plăţi sau faliment, ori declanşează procedura de lichidare, înainte de începerea prezentului contract;

c. cesionează drepturile şi obligaţiilc salc, prevăzute în prezentul contract, fără a avea acordul celeilalte părţi;

d. îşi încalcă oricare dintre obligaţiile sale după ce a fost avertizată de către cealaltă parte că o nouă încălcare a lor va atrage rezilierea contractului.

e. unilateral, prin denuntarea uneia din partile contractante, in termen de maxim 15 zile lucratoare de la data comunicarii de catre aceasta .

8.2. Partea care invocă încetarea prezentului contract are obligaţia să notifice celeilalte părţi cauza de încetare a lui cu minim 5 zile înainte de data la care aceasta urmează să-şi producă efectele.

8.3. Rezilierea contractului nu are nici un efect asupra obligaţiilor deja scadente între părţi.

8.4. Prevederile prezentului capitol nu înlătură răspunderea părţii care, în mod culpabil a cauzat încetarea contractului.

IX FORŢA MAJORĂ

9.1. Nici una dintre părţile contractante nu răspunde de neexcutarea la termen sau/şi de executarea în mod necorespunzător total sau parţial a oricărei obligaţii care îi revine în baza prezentului contract, dacă neexecutarea sau executarea necorespunzătoare a obligaţiei respective a fost cauzată de forţa majoră, aşa cum este definită de lege.

9.2. Partea care invocă forţa majoră este obligată să notifice celeilalte părţi, în termen de maximum 24 de ore producerea evenimentului şi să ia toate măsurile posibile în vederea limitării consecinţelor lui.
9.3. Dacă în termen de 48 de ore de la producere, evenimentul respectiv nu încetează, părţile au dreptul să-şi notifice încetarea de plin drept a prezentului contract fără ca vreuna dintre ele să pretindă daune-interese.

X. NOTIFICĂRI

10.1. În accepţiunea părţilor contractante, orice notificare adresată de una dintre acestea celeilalte este valabil îndeplinită dacă va fi trimisă la adresa/sediul prevăzut în partea introductivă a prezentului contract.
10.2. În cazul în care notificarea se face pe cale poştală, ea va fi transmisă, prin scrisoare recomandată, cu confirmare de primire (A.R.) şi se consideră primită de destinatar la data menţionată de oficiul poştal primitor pe această confirmare.
10.3. Dacă notificarea se trimite prin fax si/sau email, ea se consideră primită în prima zi lucrătoare după cea în care a fost expediată.
10.4. Notificările verbale nu se iau în considerare de nici una dintre părţi, dacă nu sunt confirmate, prin intermediul uneia dintre modalităţile prevăzute la alineatele precedente.

XI. LITIGII

11.1. Părţile au convenit ca toate neînţelegerile privind validitatea prezentului contract sau rezultate din interpretarea, executarea ori încetarea acestuia să fie rezolvate pe cale amiabilă de reprezentanţii lor.
11.2. În cazul în care nu este posibilă rezolvarea litigiilor pe cale amiabilă, părţile se vor adresa de comun acord Judecatoriei Sect. 1, Bucuresti

XII. CESIUNEA SI SUBCONTRACTAREA

12.1. Prestatorul are obligaţia de a nu subcontracta/cesiona contractul sau parti din acesta fara acordul prealabil dat in scris de catre Achizitor .

XIII CLAUZE CU PRIVIRE LA PROTECŢIA DATELOR CE AU CARACTER PERSONAL

13.1. Partile declara ca sunt de acord cu prelucrarea, stocarea si utilizarea datelor ce au caracter personal din cuprinsul prezentului contract conform Regulamentului (UE) 2016/679 al Parlamentului European şi al Consiliului privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor ce au caracter personal şi privind libera circulaţie a acestor date în sensul iniţierii şi derulării de raporturi juridice între acestea inclusiv în vederea îmbuntăţirii modului de comunicare prin intermediul poştei electronice, pentru comunicarea operativă şi eficientă a informaţiilor necesare .
13.2. Părţile contractante se obliga sa respecte si sa aplice intocmai prevederile legale privind prelucrarea datelor ce au caracter personal, a Regulamentul UE 2016/679 ("GDPR") pe toata durata derularii acestuia inclusiv cu privire la persoana desemnată, Prestatorului.
13.3. Partile se obliga să respecte normele şi obligaţiile impuse de dispoziţiile în vigoare, privind protecţia datelor cu caracter personal.

a) Partile sunt conştiente de faptul că normele europene din Regulamentul 679/2016 se aplică oricărui operator de date sau imputernicit situat în Uniunea Europeană şi oricărei persoane care prelucrează date cu caracter personal ale persoanelor vizate situate în Uniunea Europeană sau care le furnizează servicii. Prin urmare, Părţile confirmă respectarea deplină a următoarelor prevederi, inclusiv dar fără a se limita la:
   - ✓ capacitatea de a respecta drepturile persoanelor vizate privind ştergerea, corectarea sau transferul informaţiilor personale;
   - ✓ informarea in caz de breşă de date a tuturor destinatarilor relevanţi, într-un interval maxim de 72 ore şi, în cazul Prestatorului nu mai târziu de 24 ore de la momentul în care o astfel de încălcare a securităţii datelor a ajuns în atenţia acestuia;
   - ✓ îndeplinirea tuturor îndatoririlor obligatorii privind documentarea conformării cu Regulamentul 679/2016.
b) Părţile pot utiliza datele personale ale semnatarilor în limita contractului pe care îl au încheiat, acesta fiind baza legală a prelucrării. Orice prelucrare suplimentară sau în alt scop face obiectul unui acord separat de prelucrare a datelor, încheiat între Părţi. De asemenea perioada de stocare a datelor personale prelucrate prin contract este limitată la perioada corespondentă realizării obiectului principal al contractului.

c) Datele cu caracter personal schimbate între Părți nu pot deveni accesibile sau comunicate unor terțe părți neautorizate sau puse la dispoziție spre utilizare într-un alt mod. Prin urmare, Părțile vor lua toate măsurile tehnice și în special organizatorice necesare, în ceea ce privește obligațiile asumate prin această clauză:

- ✓ vor împiedica persoanele neautorizate să obțină acces la sistemele de prelucrarea datelor cu care sunt prelucrate sau utilizate datele cu caracter personal;
- ✓ vor preveni utilizarea fără autorizație a sistemelor de prelucrare a datelor;
- ✓ se vor asigura că persoanele care au dreptul să utilizeze un sistem de prelucrare a datelor au acces numai la datele la care au Drept de acces și că datele cu caracter personal nu pot fi citite, copiate, modificate sau eliminate fără autorizație în cursul prelucrării sau utilizării și după stocare;
- ✓ se vor asigura că datele cu caracter personal nu pot fi citite, copiate, modificate sau eliminate fără autorizație în timpul transmiterii electronice sau transportului și că este posibil să verifice și să stabilească către care organisme se dorește să se efectueze transferul datelor cu caracter personal prin mijloace de transmitere a datelor;
- ✓ se vor asigura că pot verifica și stabili dacă și de către cine au fost introduse, modificate sau eliminate datele cu caracter personal în/din sistemele de prelucrare a datelor;
- ✓ se vor asigura că, în cazul unei acțiuni de prelucrare a datelor cu caracter personal, datele sunt prelucrate strict în conformitate cu prezentul contractul incheiat între Părți;
- ✓ se vor asigura că datele cu caracter personal sunt protejate de distrugere sau pierdere accidentală;
- ✓ se vor asigura că datele colectate în scopuri diferite pot fi prelucrate separat.

XIV. CODUL DE CONDUITA

14.1. Prestatorul va acționa întotdeauna loial și imparțial și ca un consilier de încredere pentru Achizitor conform regulilor și/sau codului de conduită al profesiei sale, precum și cu respectarea confidențialității privind clauzele contractului.

14.2. Plățile către Prestator aferente contractului vor constitui singura suma ce poate deriva din prezentul contract iar Prestatorul respectiv, personalul său salariat ori contractat, inclusiv conducerea sa, nu vor accepta nici un comision, discount, alocație, plată indirectă ori orice altă formă de retribuție în legătură cu sau pentru executarea obligațiilor din prezentul contract.

14.3. Prestatorul și personalul său salariat ori contractat de acesta vor respecta confidențialitatea, pe perioada executării prezentului contract, inclusiv pe perioada oricărei prelungiri a acestuia, precum și timp de 2 ani după încetarea acestuia. În acest sens, cu excepția cazului în care se obține acordul scris prealabil al Achizitorului, Prestatorul respectiv personalul său, salariat ori contractat de acesta, incluzând conducerea, nu vor comunica timp de 2 ani oricărei alte persoane sau entități, nici o informație referitoare la prezentul contract sau despre care au luat cunoștință în perioada derulării acestuia și nu vor face publică nici o informație referitoare la recomandările primite în cursul sau ca rezultat al derulării lui. Totodată, Prestatorul, respectiv personalul său salariat ori contractat de acesta nu vor utiliza în dauna Achizitorului informațiile ce le-au fost furnizate sau rezultatul studiilor, testelor, cercetărilor desfășurate în cursul sau în scopul executării prezentului contract.

14.4. Prestatorul va transmite Achizitorului, la cerere, documente justificative cu privire la condițiile în care se execută prezentul contract.

XV. CONFLICTUL DE INTERESE

15.1. Prestatorul va lua toate măsurile necesare pentru a preveni sau stopa orice situație care ar putea compromite executarea obiectivă și imparțială a prezentului contract. Conflictele de interese pot apărea în mod special ca rezultat al intereselor economice, afinităților politice ori de naționalitate, legăturilor de rudenie ori afinitate, sau al oricăror alte legături ori interese comune. Orice conflict de interese apărut în timpul executării prezentului contract de servicii trebuie notificat în scris Achizitorului, în termen de maxim 12 ore de la apariția acestuia.

15.2. Achizitorul își rezervă dreptul de a verifica dacă măsurile luate sunt corespunzătoare și poate solicita măsuri suplimentare dacă este necesar. Prestatorul se asigură că personalul său, salariat sau contractat de el, inclusiv conducerea și salariații din teritoriu, nu se află într-o situație care ar putea genera un conflict de interese. Prestatorul se obliga sa inlocuiasca în termen de 3 zile de la constatarea conflictului de interese și fără vreo compensație din partea Achizitorului, orice membru al personalului său salariat ori contractat, inclusiv conducerea ori salariații din teritoriu, care se regăsește într-o astfel de situație.

15.3. Prestatorul trebuie sa evite orice contact care ar putea sa-i compromită independența ori pe cea a personalului său, salariat sau contractat, inclusiv conducerea și salariații din teritoriu pe perioada derulării prezentului contract. În cazul

în care Prestatorul nu-şi menţine independenţa, Achizitorul, fără afectarea dreptului acesteia de a obţine repararea prejudiciului ce i-a fost cauzat ca urmare a situaţiei de conflict de interese, va putea decide încetarea de plin drept şi cu efect imediat a prezentului contract.

15.4. Prestatorul nu are dreptul de a angaja, în scopul îndeplinirii prezentului contract, persoane fizice sau juridice care au fost implicate în procesul de verificare/evaluare a candidaturilor/ofertelor depuse în cadrul aplicării procedurii de atribuire aferentă acestuia, pe parcursul unei perioade de cel puţin 12 luni de la încheierea contractului, sub sancţiunea nulităţii contractului respectiv pentru cauză imorală.

XVI. CLAUZE FINALE

16.1. Modificarea prezentului contract se face numai prin act adiţional încheiat între părţile contractante.

16.2. Prezentul contract reprezintă voinţa părţilor şi înlătură orice altă înţelegere verbală dintre acestea, anterioară sau ulterioară încheierii lui.

16.3. În cazul în care părţile îşi încalcă obligaţiile lor, neexercitarea de partea care suferă vreun prejudiciu a dreptului de a cere executarea întocmai sau prin echivalent bănesc a obligaţiei respective nu înseamnă că ea a renunţat la acest drept al său.

16.4. Contractul are caracter de document public. Accesul persoanelor la informatiile mentionate in acesta se realizeaza cu respectarea termenelor si procedurilor prevazute de Legea nr. 544/2001 privind liberul acces la informatiile de interes public.

16.5. Prevederile prezentului contract se completează cu dispoziţiile Noului Cod Civil, Legii nr. 98/2016 privind achiziţiile publice, actualizata cu modificarile ulterioare .

16.6. Prezentul contract a fost încheiat la sediul Achizitorului astazi, 26.04.2022, in două exemplare cu valoare de original, câte una pentru fiecare parte contractanta.

ACHIZITOR
CREART - CENTRUL DE CREAȚIE, ARTĂ ȘI TRADIȚIE AL MUNICIPIULUI BUCUREȘTI

PRESTATOR

Director,

Director Adjunct (economic) .

Director Adjunct (administrativ),

Consilier Juridic,

Viza CFPP

ANEXA 1 LA CONTRACT DE SERVICII Nr. 3528/26.04.2022

SERVERE: 4 buc
STAȚII DE LUCRU:

- 114 stații PC și laptopuri PC
- 10 buc - laptop Apple
- 3 buc - Imac Apple

3. SISTEME PERIFERICE:

- 41 buc - imprimante multifuncționale
- 1 buc - fax
- 5 buc - copiatoare multifuncționale

4. NETWORK – ECHIPAMENTE ACTIVE (include operațiuni de reparare a traseelor de cablu UTP din sediul creart):

- 17 buc – switch
- 11 buc – Wifi AP pro
- 1 buc – controller wifi

Sistem proiecție sală conferință

5. SOFTWARE

- 114 buc Windows 10/Windows 10 Pro;
- 85 buc Microsoft Office (2010, 2013, 2016);
- 1 buc Windows Server 2012;
- 1 buc Linux CentOS;
- 13 buc Mac OSX;
- 11 buc Microsoft Office for MAC;
- 2 buc Photoshop CC 2022;
- 1 buc Adobe Acrobat;
- 1 buc resolume Arena

Check Point Firewall NGTX - Firewall, VPN, Advanced Networking and Clustering, Identity Awareness, Mobile Access, IPS, Application Control, URL Filtering, Anti-Virus, Anti-Bot, Anti-Spam, Content Awareness, Network Policy Management, Logging and Status, Smart Event - upgrade la ver R80.10;
Qnap NAS – sistem operare (QTS 4.3.4.), PDAP Server, SQL Server, Backup Station, Cloud Link, Qsync Central, Photo Station;
Hyper-V – hypervisor – management 3 servere virtuale; management firewall, email server linux, statie monitorizare;

Server Linux – email server;
Bitdefender Gravity Zone Cloud Console;
Antispam/Antivirus Cloud Console;

ACHIZITOR
CREART - CENTRUL DE CREATIE, ARTA SI TRADITIE AL MUNICIPIULUI BUCURESTI

PRESTATOR

Viza CFPP

Anexa 2 nr. la contract de servicii nr. 3528/26.04.2022

POLITICA DE PRELUCRARE A DATELOR FOLOSIND ECHIPAMENTE MOBILE SI LUCRUL LA DISTANTA

1 SCOP

Scopul acestui document este de a stabili reguli care să prevină accesul neautorizat la informaţiile sau resursele informatice ale Achizitorului prin intermediul tuturor tipurilor de calculatoare mobile, telefoane mobile, telefoane smart, carduri de memorie şi dispozitive mobile folosite pentru stocarea, procesarea şi transferul datelor sau folosind informaţiile stocate pe aceste echipamente aflate atât în interiorul, cât şi în exteriorul sediului Achizitorului .

2 DOMENIU DE APLICARE

Această Politică se aplică întregului Sistem de Management al Securităţii Informaţiei (SMSI): toate persoanele, datele şi echipamentele aparţinând domeniului SMSI.

Utilizatorii acestui document sunt angajaţii Achizitorului ce folosesc echipamente MCE.

3 DEFINIŢII ŞI PRESCURTĂRI

3.1 Definiţii

Securitatea informaţiei - păstrarea confidenţialităţii, integrităţii şi disponibilităţii informaţiei.
Echipament MCE - include toate tipurile de calculatoare mobile, telefoane mobile, telefoane smart, carduri de memorie şi dispozitive mobile folosite pentru stocarea, procesarea şi transferul datelor.

3.2 Prescurtări

RGPD = Regulament general privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date.

4 DOCUMENTE DE REFERINŢĂ ŞI CONEXE

- REGULAMENTUL (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.
- Politica în domeniul securităţii informaţiei
- Politica în domeniul transferului de informaţii
- Evaluarea resurselor informaţionale
- Metodologia de evaluare a riscurilor asociate resurselor informaţionale

5 RESPONSABILITĂŢI

- Responsabilul de Securitate numit de Director mentine Politica de Securitate si furnizeaza asistenta in vederea aplicarii.
- Responsabilitatea reviziei acestui document revine Responsabilului echipei de securitate şi suport – o dată pe an.
- Directorul aplica, impune si mentine permanent aceasta Politica de Securitate in aria de acoperire a SMSI.

Anexa 2 nr. la contract de servicii nr. 3528/26.04.2022

POLITICA DE PRELUCRARE A DATELOR FOLOSIND ECHIPAMENTE MOBILE SI LUCRUL LA DISTANTA

În evaluarea eficienţei şi compatibilităţii prezentului document trebuie să se ţină cont de următoarele criterii:

- Numărul incidentelor legate de deplasarea echipamentului MCE în afara perimetrului sediului Achizitorului fără autorizaţie;
- Numărul incidentelor legate de accesul neautorizat la echipamente MCE în afara perimetrului sediului Achizitorului .
- Toti responsabilii numiti in cadrul sediului Achizitorului au directa raspundere de a implementa aceasta politica de securitate in cadrul ariilor de activitate alocate.
- Fiecare angajat/Prestator de servicii al Achizitorului adera la aceasta politica de securitate. Responsabilitatile de securitate revin tuturor angajatilor/ Prestatorilor de servicii si se fac cunoscute in descrierea postului.

6 DESCRIEREA ACTIVITĂŢILOR

REGULI PRIVIND UTILIZAREA MCE

O atenţie deosebită ar trebui acordată atunci când echipamentul MCE este plasat în vehicule (inclusiv autoturisme), spaţii publice, camere de hotel, centre de conferinţă şi alte zone neprotejate din afara perimetrului Achizitorului .

Persoana care scoate în afara perimetrului Achizitorului echipamentul MCE trebuie să respecte următoarele reguli:

- echipamentul MCE care conţine informaţii importante, sensibile sau critice, nu trebuie lăsat nesupravegheat şi, în măsura în care este posibil, trebuie bine securizat fizic;
- când echipamentul MCE este folosit în locuri publice, utilizatorul său trebuie să se asigure că datele nu pot fi accesate de persoane neautorizate;
- instalarea/ actualizarea de patch-uri ale sistemului de operare şi ale aplicaţiilor este realizată de persoane autorizate;
- protecţia împotriva virusurilor este instalată şi actualizată de echipa de securitate şi suport IT;
- persoana care utilizează echipamentul MCE în afara perimetrului Achizitorului este responsabilă de realizarea cu regularitate a procesului de back-up al datelor
- conectarea la informaţiile sau sistemele de informaţii, la reţele Achizitorului şi transferul datelor se vor efectua respectând prevederile legale.

- Informaţia stocată pe calculatoare portabile trebuie să fie criptată în conformitate cu evaluările informaţiei folosind prevederile Politicii de Securitate a sistemului Resurselor Informatice. Responsabilul cu protecţia datelor si prestatorul de servicii ce asigura menetenta echipamentelor IT se asigură de instruirea şi conştientizarea persoanelor care folosesc echipamente MCE în afara perimetrului Achizitorului .

Anexa nr. 3 la contract de servicii nr. 3528/26.04.2022

POLITICA DE UTILIZARE A RESURSELOR INFORMATICE

1. SCOP

Scopul acestui document este de a stabili reguli clare privind folosirea sistemelor de informații și a altor resurse informatice la sediul Achizitorului.

2. DOMENIU

Acest document se aplică întregului domeniu al SMSI Achizitorului/CREART
Prevederile acestui document se aplică întregului personal al CREART.

3. DEFINIȚII ȘI PRESCURTĂRI

3.1 Definiții
Sistemul informatic- include toate serverele și colaboratorii aferenți, structura de rețele, aplicațiile software sau de rețea, bazele de date, și toate subsistemele de calculatoare sau componente deținute de Achizitor sau care se află sub responsabilitatea Achizitorului.
Folosirea sistemului informatic include folosirea oricărui serviciu intern sau extern (facilitat de sistemul informatic) cum ar fi folosirea Internetului, a e-mailului, etc.
Resursele informatice - reprezintă toate sistemele informatice și alte echipamente ce utilizează informația cum ar fi documentele pe suport de hârtie, telefoanele mobile, laptopurile, mediile de stocare mobile etc.
Securitatea informației - păstrarea confidențialității, integrității și disponibilității informației.
3.2 Prescurtări
RGPD - Regulament general privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date
CREART = institutie.
SMSI - SISTEMUL DE MANAGEMENT AL SECURITĂȚII INFORMATICE

4. DOCUMENTE DE REFERINȚĂ ȘI CONEXE

- REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date.
- CLASIFICAREA RESURSELOR INFORMAȚIONALE
- MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMAȚIEI
- INVENTARIEREA RESURSELOR INFORMAȚIONALE
- PRELUCRAREA DATELOR FOLOSIND ECHIPAMENTE MOBILE ȘI LUCRUL LA DISTANȚĂ
- POLITICA PRIVIND CONTROLUL ACCESULUI
- Regulament intern al CREART

5. RESPONSABILITĂȚI

DPO cu ajutorul si societatii externalizata de servicii mentenanta a infrastructurii IT .
La evaluarea compatibilității și eficienței acestei Politici se vor lua în considerare următoarele criterii:
- numărul evenimentelor de securitate înregistrate ca urmare a folosirii inacceptabile (abuzivă) sau neautorizată a resurselor informatice
- numărul evenimentelor de securitate înregistrate ca urmare a lipsei de instruire corespunzătoare a personalului privind utilizarea resurselor informatice sau a lipsei de conștientizare a importanței subiectului.

6 DESCRIEREA ACTIVITĂȚILOR

6.1 REGULI PRIVIND UTILIZAREA RESURSELOR INFORMATICE
a. Resursele informatice pot fi folosite doar în scopul îndeplinirii sarcinilor de serviciu
b. Fiecare resursă informatică are un deținător așa cum este precizat in Inventarul resurselor informatice în conformitate cu "INVENTARIEREA RESURSELOR INFORMAȚIONALE". Deținătorul resursei informatice este responsabil pentru păstrarea securității resursei respective.

c. Este interzisă folosirea resurselor informatice într-o manieră care:
- să solicite nejustificat resursele sistemelor informatice,
- să testeze slăbiciuni/vulnerabilități ale sistemelor informatice
- să conducă la potențiale amenințări informatice

Sunt interzise de asemenea următoarele :

- descărcarea fișierelor imagini sau video care nu au legătură cu activitatea CREART
- instalarea de software pe un computer local fără acceptul echipei de securitate și suport IT
- descărcarea de aplicații Java, controale Active X sau alte coduri mobile fără acceptul echipei de securitate și suport IT
- descărcarea de cod sursă al programelor de pe medii externe de stocare fără acceptul echipei de securitate și suport IT
- instalarea sau folosirea echipamentelor periferice cum ar fi modemurile, cârdurile de memorie și alte dispozitive pentru arhivarea sau citirea datelor fără acceptul echipei de securitate și suport IT

d. Folosirea resurselor informatice în exteriorul CREART se supune prevederilor din "PRELUCRAREA DATELOR FOLOSIND ECHIPAMENTE MOBILE ȘI LUCRUL LA DISTANȚĂ"

e. La incetarea contractelor de muncă sau de altă natură toate resursele informatice se returnează CREART în conformitate cu prevederile "ÎNCETAREA_ȘI_SUSPENDAREA_CONTRACTULUI_DE_MUNCĂ" și " POLITICA PRIVIND CONTROLUL ACCESULUI "

f. Păstrarea informațiilor se realizează în conformitate cu prevederile "PROCEDURA_DE_BACK-UP"

g. Accesul la sistemele informatice se realizează în conformitate cu prevederile POLITICA PRIVIND CONTROLUL ACCESULUI

h. Utilizarea echipamentului de calcul inclusiv accesul la Internet și la e-mail se realizează în conformitate cu prevederile UTILIZAREA RESURSELOR INFORMATICE și respectând condițiile prevăzute în Regulamentul Intern al CREART în vigoare.

i. Evenimentele sau incidentele de securitate se gestionează conform revederilor MANAGEMENTUL INCIDENTELOR DE SECURITATE A INFORMAȚIEI

7 ÎNREGISTRĂRI

8 ANEXE -Nu sunt

Anexa 4 la contract de servicii nr. 3528/26.04.2022

POLITICA IN RELAȚIILE CU TERTII

Operatorul și persoana împuternicită de operator. GDPR Articolul 28. Persoana împuternicită de operator

(1) În cazul în care prelucrarea urmează să fie realizată în numele unui operator, operatorul recurge doar la persoane împuternicite care oferă garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să respecte cerințele prevăzute în prezentul regulament și să asigure protecția drepturilor persoanei vizate.

(2) Persoana împuternicită de operator nu recrutează o altă persoană împuternicită de operator fără a primi în prealabil o autorizație scrisă, specifică sau generală, din partea operatorului. În cazul unei autorizații generale scrise, persoana împuternicită de operator informează operatorul cu privire la orice modificări preconizate privind adăugarea sau înlocuirea altor persoane împuternicite de operator, oferind astfel posibilitatea operatorului de a formula obiecții față de aceste modificări.

(3) Prelucrarea de către o persoană împuternicită de un operator este prevazuta in contract sau alt act juridic în temeiul dreptului Uniunii sau al dreptului intern care are caracter obligatoriu pentru persoana împuternicită de operator în raport cu operatorul și care stabilește obiectul și durata prelucrării, natura și scopul prelucrării, tipul de date cu caracter personal și categoriile de persoane vizate și obligațiile și drepturile operatorului. Respectivul contract sau act juridic prevede în special că persoană împuternicită de operator:
(a) prelucrează datele cu caracter personal numai pe baza unor instrucțiuni documentate din partea operatorului, inclusiv în ceea ce privește transferurile de date cu caracter personal către o țară terță sau o organizație internațională, cu excepția cazului în care această obligație îi revine persoanei împuternicite în temeiul dreptului Uniunii sau al dreptului intern care i se aplică; în acest caz, notifică această obligație juridică operatorului înainte de prelucrare, cu excepția cazului în care dreptul respectiv interzice o astfel de notificare din motive importante legate de interesul public;
(b) se asigură că persoanele autorizate să prelucreze datele cu caracter personal s-au angajat să respecte confidențialitatea sau au o obligație statutară adecvată de confidențialitate;
(c) adoptă toate măsurile necesare în conformitate cu articolul 32;
(d) respectă condițiile menționate la alineatele (2) și (4) privind recrutarea unei alte persoane împuternicite de operator;
(e) ținând seama de natura prelucrării, oferă asistență operatorului prin măsuri tehnice și organizatorice adecvate, în măsura în care acest lucru este posibil, pentru îndeplinirea obligației operatorului de a răspunde cererilor privind exercitarea de către persoana vizată a drepturilor prevăzute în capitolul III;
(f) ajută operatorul să asigure respectarea obligațiilor prevăzute la articolele 32-36, ținând seama de caracterul prelucrării și informațiile aflate la dispoziția persoanei împuternicite de operator;

(g) la alegerea operatorului, șterge sau returnează operatorului toate datele cu caracter personal după încetarea furnizării serviciilor legate de prelucrare și elimină copiile existente, cu excepția cazului în care dreptul Uniunii sau dreptul intern impune stocarea datelor cu caracter personal;

(h) pune la dispoziția operatorului toate informațiile necesare pentru a demonstra respectarea obligațiilor prevăzute la prezentul articol, permite desfășurarea auditurilor, inclusiv a inspecțiilor, efectuate de operator sau alt auditor mandatat și contribuie la acestea.

În ceea ce privește primul paragraf litera (h), persoana împuternicită de operator informează imediat operatorul în cazul în care, în opinia sa, o instrucțiune încalcă prezentul regulament sau alte dispoziții din dreptul intern sau din dreptul Uniunii referitoare la protecția datelor.

(4) În cazul în care o persoană împuternicită de un operator (numai cu acordul in scris al Achizitorului) recrutează o altă persoană împuternicită pentru efectuarea de activități de prelucrare specifice în numele operatorului, aceleași obligații privind protecția datelor prevăzute în contractul sau în alt act juridic încheiat între operator și persoana împuternicită de operator, astfel cum se prevede la alineatul (3), revin celei de a doua persoane împuternicite, prin intermediul unui contract sau al unui alt act juridic, în temeiul dreptului Uniunii sau al dreptului intern, în special furnizarea de garanții suficiente pentru punerea în aplicare a unor măsuri tehnice și organizatorice adecvate, astfel încât prelucrarea să îndeplinească cerințele prezentului regulament. În cazul în care această a doua persoană împuternicită nu își respectă obligațiile privind protecția datelor, persoana împuternicită inițială rămâne pe deplin răspunzătoare față de operator în ceea ce privește îndeplinirea obligațiilor acestei a doua persoane împuternicite.

(5) Aderarea persoanei împuternicite de operator la un cod de conduită aprobat, menționat la articolul 40, sau la un mecanism de certificare aprobat, menționat la articolul 42, poate fi utilizată ca element prin care să se demonstreze existența garanțiilor suficiente menționate la alineatele (1) și (4) din prezentul articol.

(6) Fără a aduce atingere unui contract individual încheiat între operator și persoana împuternicită de operator, contractul sau celălalt act juridic menționat la alineatele (3) și (4) din prezentul articol se poate baza, integral sau parțial, pe clauze contractuale standard menționate la alineatele (7) și (8) din prezentul articol, inclusiv atunci când fac parte dintr-o certificare acordată operatorului sau persoanei împuternicite de operator în temeiul articolelor 42 și 43.

(7) Comisia poate să prevadă clauze contractuale standard pentru aspectele menționate la alineatele (3) și (4) din prezentul articol și în conformitate cu procedura de examinare menționată la articolul 93 alineatul (2).

(8) O autoritate de supraveghere poate să adopte clauze contractuale standard pentru aspectele menționate la alineatele (3) și (4) din prezentul articol și în conformitate cu mecanismul pentru asigurarea coerenței menționat la articolul 63.

(9) Contractul sau celălalt act juridic menționat la alineatele (3) și (4) se formulează în scris, inclusiv în format electronic.

(10) Fără a aduce atingere articolelor 82, 83 și 84, în cazul în care o persoană împuternicită de operator încălcă prezentul regulament, prin stabilirea scopurilor și mijloacelor de prelucrare a datelor cu caracter personal, persoana împuternicită de operator este considerată a fi un operator în ceea ce privește prelucrarea respectivă.

În cazul în care rolul terțului este de a prelucra date cu caracter personal pentru sau în numele Achizitorului înainte de a furniza date cu caracter personal către terți sau de a implica un terț:
(1) vom realiza o verificare prealabilă a confidențialității pentru a evalua practicile de confidențialitate și riscurile asociate cu acești terți,
(2) vom obține din partea terților respectivi asigurări contractuale că vor :

- prelucra datele cu caracter personal doar conform instrucțiunilor Achizitorului și în conformitate cu prezenta politică, inclusiv, dar fără limitare la toate cele 8 principii privind confidențialitatea și celelalte standarde stabilite în prezenta politică și legislația aplicabilă,
- notifica Achizitorul cu promptitudine cu privire la orice incident privind confidențialitatea, inclusiv orice incapacitate de a se conforma cu standardele stabilite în această politică și cu legislația aplicabilă, sau incident de securitate,
- coopera pentru remedierea promptă a oricărui incident materializat și pentru abordarea drepturilor individuale prevăzute,

- că nu vor angaja altă societate pentru a prelucra datele cu caracter personal, fără autorizația scrisă din partea Achizitorului sau fără a implementa un acord care să impună obligații echivalente privind protecția datelor,
- vor șterge sau ne vor returna toate datele cu caracter personal, după ce au încheiat furnizarea de servicii către noi sau la cererea Achizitorului și că vor permite institutiei noastre să verifice și să monitorizeze practicile lor pentru durata prelucrării, în scopul respectării acestor cerințe.

În plus, în cazul în care terțul prelucrează date cu caracter personal care provin dintr-o țară sau un teritoriu cu o lege care limitează comunicarea unor astfel de date, ne vom asigura că transmiterea către terț îndeplinește cerințele pentru transferul transfrontalier de informații .

În situația în care rolul terțului este de a furniza institutiei noastre date cu caracter personal, înainte de a obține astfel de date de la terțul în cauză, ne vom asigura că sunt îndeplinite cerințele de transparență pentru colectarea datelor cu caracter personal din alte surse și nu în mod specific sub îndrumarea companiei noastre și vom obține declarații contractuale din partea terțului că nu încalcă nicio lege sau drepturile oricărei terțe părți prin furnizarea către compania noastră a unor date cu caracter personal.

Dacă rolul terțului este de a primi de la noi informații pentru prelucrare care nu se realizează în mod specific sub îndrumarea institutiei noastre, înainte de a furniza informații terțului, ne vom asigura că informațiile au fost depersonalizate și vom obține garanții scrise din partea terțului că le va folosi numai în scopuri definite în acord și în conformitate cu legislația aplicabilă și că nu va încerca să reidentifice informațiile.

Dacă transferul către o terță parte este necesar pentru a proteja interesele legitime ale persoanei fizice sau ale institutiei, informațiile pot fi transferate: (1) pentru a preveni frauda sau pentru a aplica sau proteja drepturile și bunurile institutiei ,(2) pentru protejarea siguranței personale a angajaților Achizitorului sau părților terțe, (3) pentru a proteja bunurile Achizitorului prin adoptarea de măsuri corective de securitate, dacă suspectăm, în mod rezonabil, că au avut loc activități ilegale sau abateri grave.

Anexa 5 la la contract de servicii nr. 3528/26.04.2022

POLITICA PRIVIND PAROLAREA

1 SCOP

Scopul acestui document este de a defini un set de reguli necesare gestionării sigure a parolelor în cadrul SISTEMULUI DE MANAGMENT AL SECURITĂŢII INFORMATICE (SMSI) al Achizitorului.

2 DOMENIU

Această Politică se aplică întregului SMSI (ex. toate sistemele, echipamentele, facilităţile şi informaţiile folosite în SMSI). Utilizatorii acestui document sunt toţi angajaţii Achizitorului .

3 DEFINIŢII ŞI PRESCURTĂRI

3.1 Definiţii

Securitatea informaţiei - păstrarea confidenţialităţii, integrităţii şi disponibilităţii informaţiei.

3.2 Prescurtări

RGPD = Regulament general privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date
SMSI (SISTEMUL DE MANAGMENT AL SECURITĂŢII INFORMATICE ex. toate sistemele, echipamentele, facilităţile şi informaţiile folosite în SMSI).

4 DOCUMENTE DE REFERINŢĂ ŞI CONEXE

REGULAMENTUL (UE) 2016/679 AL PARLAMENTULUI EUROPEAN ŞI AL ONSILIULUI din 27 aprilie 2016 privind protecţia persoanelor fizice în ceea ce priveşte prelucrarea datelor cu caracter personal şi privind libera circulaţie a acestor date.

MANAGEMENTUL INCIDENTELOR DE SECURITATEA INFORMAŢIEI

5 RESPONSABILITĂŢI

Responsabilul echipei de securitate şi suport IT verifică şi eventual modifică acest document o dată pe an si/sau ori de cate ori este nevoie .

La evaluarea compatibilităţii şi eficienţei acestei Politici se vor lua în considerare următoarele criterii:

- numărul incidentelor legate de folosirea greşită a parolelor de către persoanele neautorizate
- numărul incidentelor legate de gestionarea inadecvată a parolelor.

6 DESCRIEREA ACTIVITĂŢILOR. MANAGEMENTUL PAROLELOR ÎN ACHIZITORULUI/CREART

6.1 Reguli de bună practică

Tot personalul Achizitorului trebuie să aplice următoarele reguli de bună practică în situaţia în care accesul la o activitate sau document este parolat în vederea asigurării securităţii informaţiei :

- parolele nu trebuie dezvăluite altor persoane, inclusiv conducerii şi administratorilor de sistem;
- parolele nu trebuie scrise pe suport fizic;
- parolele generate de utilizator nu trebuie distribuite sub nicio formă (oral, scris sau electronic);
- parolele trebuie schimbate dacă există indicii ca acestea sau sistemul au fost compromise –în cazul acesta trebuie raportat incidentul de securitate conform PROCEDURII – MANAGEMENTUL INCIDENTELOR DE SECURITATE ALE INFORMAŢIEI;
- parola trebuie schimbată o dată la 3 luni;
- parola trebuie schimbată la prima înregistrare în sistem;
- parolele utilizate în scopuri personale nu trebuie folosite în activităţile de serviciu;
- parolele nu ar trebui să aibă semnificaţie personală (ex. data naşterii, adresa, nume ale membrilor de familie etc.);
- ultimele 3 parole nu trebuie refolosite;

Trebuie selectate parole cat mai sigure, iar în alegerea acestora este recomandat să se ţină seama de:

- folosirea cel puţin a 8 caractere;
- folosirea cel puţin a 2 caractere numerice;
- folosirea cel puţin a unui caracter alfabetic mare şi a cel puţin unui caracter alfabetic normal;
- folosirea cel puţin a unui caracter special;
- parola nu trebuie să fie un cuvânt sau jargon din dicţionar, din orice limbă, sau oricare dintre acestea scrise invers.

6.2 Sistemul de management al parolei în CREART

Aprobarea de către Director a Declaraţiei de Confidentialitate implică acceptarea utilizatorilor Achizitorului a obligativităţii privind păstrarea confidenţialităţii informaţiilor.
Responsabilul echipei de securitate şi suport IT asigură respectarea următoarelor reguli în ceea ce priveşte utilizarea parolelor în CREART :

- fiecare utilizator poate folosi numele de utilizator unic alocat;
- fiecare utilizator trebuie să aibă posibilitatea să-şi aleagă propria parola, acolo unde se poate;
- parola temporară utilizată pentru prima înregistrare în sistem trebuie să fie unică şi sigură, aşa cum este menţionat mai sus;
- parolele temporare trebuie comunicate utilizatorului într-o formă sigură;
- sistemul de management al parolei trebuie să solicite utilizatorului să schimbe parola temporară la prima înregistrare în sistem;
- sistemul de management al parolei trebuie să solicite utilizatorului să aleagă parole sigure;
- sistemul de management al parolei trebuie să solicite utilizatorului să modifice parola la fiecare 3 luni;
- dacă utilizatorul solicită o nouă parolă, sistemul de management al parolei trebuie să

determine identitatea utilizatorului;

- parola nu trebuie să fie vizibilă pe ecranul calculatorului în timpul înregistrării;
- dacă un utilizator introduce incorect parola de 3 ori consecutiv, sistemul trebuie să blocheze contul utilizatorului respectiv;
- parola creată de producătorul software-ului sau hardware-ului trebuie schimbată în timpul instalării inițiale;
- fișierele care conțin parole trebuie salvate separat de aplicațiile sistemului de date.

Anexa 6 la contract de servicii nr. 3528/26.04.2022

POLITICA IN DOMENIUL TRANSFERULUI DE INFORMAȚII

I. Introducere

Prin „transfer de date cu caracter personal”, înțelegem divulgarea datelor din una sau mai multe organizații către o societate terță parte sau mai multe, precum și transferul de date între diferite entități ale unei organizații. Transferul de date poate lua forma unui transfer de date repetitiv, de rutină, caz în care are loc transferul aceluiași set de date între aceleași organizații pentru un anume scop sau transferul de date nerepetitiv/ad-hoc care se poate efectua în baza unor decizii de transfer al a datelor, fiind nerepetitiv, și care se referă doar la un număr limitat de persoane vizate.

Regulamentul acoperă, așadar, două mari tipuri de transfer de date:– Transferul repetitiv de date, de rutină, în cazul în care aceleași seturi de date sunt transferate între aceleași organizații pentru un scop stabilit. Acesta ar putea implica un grup de organizații care încheie un acord de transfer de date reciproc în vederea prelucrării datelor în scopuri specifice;

– Transferul de date nerepetitiv sau ad-hoc, efectuat în baza unei decizii de transfer. O mare parte dintre situațiile de transfer de date au loc într-un mod pre-planificat și de rutină în baza unor norme și proceduri. Cu toate acestea, organizațiile pot decide, de asemenea, sau pot solicita, să se efectueze un transfer al datelor în situații care nu sunt acoperite de un acord de transfer a datelor de rutină. În unele cazuri, acesta poate implica o decizie cu privire la transferul de date, care să prevadă condițiile reale de urgență în care a fost efectuat.

GDPR face o distincție între transferul de date efectuat de către un operator de date cu alt operator, și transferul efectuat de către un operator de date către o persoană împuternicită. În situația în care operatorul de date prelucrează date cu caracter personal cu ajutorul unei persoane împuternicite, trebuie să se asigure în cadrul unui raport contractual (în scris) faptul că:– persoana împuternicită acționează numai la instrucțiunile operatorului de date; și– există asigurate condițiile de securitate adecvate, echivalente cu cele impuse de către operatorul de date.

1. Transferul datelor cu caracter personal către o persoană împuternicită

Deși transferul de date are loc, în principal, între operatorii de date, situație în care ambele organizații stabilesc scopurile pentru care și modul în care sunt prelucrate datele personale, suntem în prezența unui transfer al datelor cu caracter personal și în cazul în care un operator transferă date cu o altă parte, care prelucrează date cu caracter personal în numele său. Aceste organizații sunt cunoscute sub denumirea de persoane împuternicite.

2. Transferul datelor cu caracter personal în cadrul organizațiilor/între operatori

În general, când vorbim despre „transferul de date“, cel mai des se va înțelege acest lucru ca fiind transferul de date efectuat între organizații. În orice caz, principiile privind protecția datelor cu caracter personal se aplică în aceeași măsură transferului de informații în cadrul unei organizații.- de exemplu, între diferitele departamente ale unei organizații / autorități sau entități .

Aspecte privind decizia de transfer a datelor cu caracter personal. În momentul adoptării deciziei de transfer operatorul de date cu caracter personal va avea în vedere următoarele:

– Care este scopul acestui transfer? Operatorul va trebui să aibă o reprezentare clară a scopului, sau a setului de obiective. Având această reprezentare, va putea ști ce date are nevoie să transfere și cu cine. Ca recomandare de bună practică ar fi bine să poată demonstra această documentare;

– **Ce informații trebuie transferate?** Nu ar trebui să transfere toate datele cu caracter personal pe care le deține ci doar anumite date necesare pentru a-și atinge obiectivele. De exemplu, operatorul ar putea avea nevoie să transfere numele și adresa unei anumite persoane, nu și alte informații pe care le deține despre acea persoană;

Cine va avea acces la datele transferate? Doar organizațiile care au nevoie de datele personale ar trebui să aibă acces la datele transferate și numai personalul relevant din cadrul acestor organizații. Acest lucru ar trebui să abordeze, de asemenea, orice restricții necesare ale transferului de date, pe mai departe, cu terțe părți;

Când ar trebui transferate datele? Ca bună practică este recomandată documentarea în acest sens, de exemplu stabilind dacă transferul ar trebui să fie un proces continuu, de rutină sau dacă ar trebui să aibă loc ca răspuns la anumite evenimente particulare;

– **Cum ar trebui să fie transferate datele?** Acest lucru implică abordarea securității din jurul transmiterii sau accesării datelor și stabilirea unor reguli comune de securitate;

– **Cum putem verifica dacă transferul atinge scopul preconizat?** Operatorul va trebui să analizeze dacă este încă necesar și de a confirma că garanțiile se potrivesc încă riscurilor;

– **Ce riscuri presupune transferul datelor cu caracter personal?** De exemplu, există vreo persoană care ar putea fi afectată de transfer? Există vreo persoană care ar putea obiecta? Ar putea submina încrederea persoanelor în organizațiile care dețin înregistrări ale datelor cu caracter personal?

– **Ar putea ca scopul să fie atins fără transferul datelor sau prin anonimizarea lor?** Nu este potrivit să se utilizeze datele cu caracter personal pentru a planifica prestarea serviciului, de exemplu, în cazul în care acest lucru ar putea fi realizat cu informații care nu se ridică la nivelul datelor cu caracter personal;

– **Are nevoie operatorul să își actualizeze notificarea?** Trebuie să se asigure că transferul este acoperit în registrul de intrări.

În concluzie, înainte de a transfera date cu caracter personal pe care le deține operatorul, va trebui să ia în considerare toate implicațiile juridice. Capacitatea operatorului de a transfera date este condiționată de o serie de constrângeri legale de protecție a datelor. De asemenea, pot exista alte considerații, cum ar fi anumite interdicții legale în privința transferului, restricții privind drepturile de autor sau o îndatorire de păstrare a confidențialității, care poate afecta capacitatea operatorului de a transfera datele cu caracter personal. Obligația de confidențialitate poate fi menționată în mod expres sau poate fi implicită, în funcție de natura informațiilor sau dacă acestea au fost colectate în condiții de confidențialitate – de exemplu, informații medicale sau informații bancare.

Anexa 7 la contract de servicii nr. **3528/26.04.2022**

PROCEDURA DE MANAGEMENT AL INCIDENTELOR DE SECURITATE A INFORMAŢIEI

1. SCOP

Scopul acestui document este de a asigura identificarea şi raportarea evenimentelor sau incidentelor de securitate a informaţiilor şi de a avea o reacţie rapidă în cazul apariţiei acestora.

2. DOCUMENTE DE REFERINŢĂ

- REGULI PRIVIND SECURITATEA REŢELEI DE CALCULATOARE
- REGULAMENTUL DE ORDINE INTERIOARĂ

3. DOMENIU DE APLICARE

Prevederile acestei proceduri se aplică tuturor resurselor informaţionale din CREART , de către personalul institutiei şi al terţelor părţi care intră în contact cu aceste resurse.

4. DEFINIŢII

Ameninţare - orice potenţial eveniment care poate cauza prejudicii institutiei

Vulnerabilitate - o slăbiciune a unei resurse sau grup de resurse, care poate fi exploatată de una sau mai multe ameninţări

Eveniment de securitate - situaţie identificată în legătură cu un sistem, un serviciu sau o reţea care indică o posibilă încălcare a politicii de securitate, un eşec al măsurilor de protecţie sau o situaţie ignorată anterior dar relevantă din punct de vedere al securităţii informaţiei.
Incident de securitate - un eveniment sau o serie de evenimente de securitate care au o probabilitate semnificativă de a compromite activităţile socităţii şi de a aduce ameninţări la securitatea informaţiei.

5. MOD DE LUCRU SI REŞPONSABILITĂŢI

5.1. Identificarea vulnerabilităţilor, evenimentelor şi incidentelor privind securitatea informaţiilor

Orice angajat alAchizitorului sau al unei părţi interesate, care este în contact cu informaţiile şi/sau sistemele informaţionale ale Achizitorului trebuie să raporteze vulnerabilităţile, evenimentele sau incidentele, după cum urmează:

- cele legate de IT&C, în conformitate cu prevederile procedurii
- cele legate de protecţia fizică şi controlul accesului.

Vulnerabilităţile, evenimentele sau incidentele identificate trebuie raportate cât mai repede posibil (telefonic sau personal). Raportarea trebuie să conţină următoarele detalii:

- tipul de neconformitate sau încălcare;
- tipul de disfuncţionalitate;
- descrierea şi zona de apariţie;
- comportament neobişnuit.

Printre evenimentele şi incidentele de securitate a informaţiei, se pot enumera următoarele:

- disfunctionalităţi ale serviciului, echipamentelor sau facilităţilor;
- supraîncărcări ale sistemului informatic;
- erori umane;
- neconformitatea cu politicile / procedurile / instrucţiunile Achizitorului;
- încălcarea politicilor / procedurilor / instrucţiunilor de securitate fizică;
- disfunctionalităţi ale software-lui sau hardware-ului;

Notă: Niciun angajat al Achizitorului sau al unei terţe părţi interesate, care este în contact cu informaţiile si/sau sistemele informaţionale ale Achizitorului nu are voie să încerce să confirme existenţa vulnerabilităţilor de securitate identificate/suspectate. Testarea vulnerabilităţilor poate fi interpretată ca o utilizare abuzivă şi poate să atragă răspunderea legală asupra persoanei care a efectuat testarea.

5.2. Clasificarea vulnerabilităţilor, evenimentelor şi incidentelor privind securitatea informaţiei

Funcţia înştiinţată înregistrează informaţia primită în "Registrul de Evidenţă a Incidentelor" şi apoi o clasifică în:

- Vulnerabilitate sau eveniment de securitate - poate conduce la apariţia unui incident de securitate
- Incident minor - un incident fără impact semnificativ asupra confidenţialităţii şi integrităţii informaţiei, care nu poate cauza indisponibilitatea informaţiei pe termen lung;
- Incident major - un incident care poate produce pierderi semnificative, datorită pierderii confidenţialităţii şi integrităţii informaţiei, sau care poate conduce la întreruperi în disponibilitatea informaţiei şi/sau a proceselor pentru o perioadă de timp incompatibilă cu funcţionarea normală a Achizitorului .

5.3. Modalităţile de rezolvare pentru vulnerabilităţile / evenimentele / incidentele de securitate

Responsabilul DPO / Directorul Achizitorului analizează informaţia înregistrată, stabileşte cauza şi decide măsurile ce se impun a fi luate, cu consultarea şi obţinerea aprobării factorilor de decizie, atunci când este necesar (ex.: la alocarea de resurse suplimentare, la noi achiziţii etc.).

Semestrial/ori de câte ori este nevoie în urma incidentelor majore, Responsabilul IT&C / , Directorul analizează informaţiile înregistrate în "Registrul de evidenţă incidente de securitate" şi monitorizează eficacitatea măsurilor dispuse.

5.4. Acţiunile disciplinare

6. Pentru incidentele ce ţin de reţeaua de calculatoare a Achizitorului, se aplică măsurile disciplinare documentate în regulamente.

7. Pentru celelalte tipuri de incidente, se acţionează conform Regulament intern al Achizitorului / prevederile legale aplicabile în vigoare.

7.1. Colectarea probelor

In cazul în care o acţiune împotriva unei persoane sau a unei organizaţii, dispusă în urma unui incident de securitate, implică o acţiune legală (civilă sau penală), DPO / Directorul CREART, împreună, stabilesc regulile de identificare, colectare şi păstrare a probelor în conformitate cu legislaţia aplicabilă în vigoare.

8. GESTIONAREA ÎNREGISTRĂRILOR GENERATE DE APLICAREA ACESTUI DOCUMENT

"Registrul de evidenţă vulnerabilităţi/evenimente / incidente de securitate" (varianta în vigoare), păstrat în format electronic în calculatoarele DPO / Directorului CREART. Documentul este arhivat pe o perioadă de 3 ani.

Regulile de identificare, colectare şi păstrare a probelor sunt păstrate în format electronic, în calculatorul DPO, unde sunt arhivate pentru o perioadă de 5 ani.

9. CRITERIILE DE EVALUARE ALE EFICIENŢEI

La evaluarea eficienţei şi adecvării acestui document se foloseşte criteriul: numărul de neconformităţi de la prevederile acestei proceduri, identificate anual.

Anexa 8 la contract de servicii nr. 3528/26.04.2022

POLITICA DE SECURITATE PRIVIND SISTEMUL RESURSELOR INFORMATICE ŞI DE COMUNICAŢII

1.1 Introducere

În acord cu prevederile din prezentul document, **R**esursele **I**nformatice şi de **C**omunicaţii (RIC) sunt bunuri strategice ale Achizitorului /CREART.

Compromiterea securităţii sistemului RIC poate afecta capacitatea Achizitorului de a oferi serviciile specifice, poate conduce la fraude sau distrugerea datelor, violarea clauzelor contractuale, divulgarea secretelor, afectarea credibilităţii Achizitorului /CREART.

Această politică este stabilită astfel încât:

- Să fie în conformitate cu statutul, regulamentele, legile şi alte documente oficiale în vigoare privind administrarea resurselor informatice;
- Să stabilească practici prudente şi acceptabile privind utilizarea RIC ale Achizitorului ./CREART;
- Să instruiască utilizatorii care au dreptul de folosire a sistemului RIC privind responsabilităţile asociate unei astfel de utilizări;

Politica de securitate a sistemului RIC al Achizitorului/CREART se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la orice resursă informatică şi de comunicaţii (a Achizitorului /CREART).

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

- Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- Colaboratorii Achizitorului /CREART care au acces la sistemul RIC;
- Operatorii economici ai Achizitorului /CREART care au acces la sistemul RIC;
- Alte persoane, entităţi sau organizaţii care au acces la sistemul RIC conform prevederilor legale.

1.2 Scopul politicii de securitate

Având în vedere că majoritatea personalului instituţiei este familiarizat cu termenii tehnici şi de asemenea cunosc sistemul de operare Windows şi pachetul de programe Microsoft Office politica de securitate a sistemului RIC are ca scop asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei.

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 Achizitorului/CREART, sunt proprietatea instituţiei în condiţiile legilor în vigoare. Utilizatorul răspunde personal de confidenţialitatea datelor încredinţate prin procedurile de acces la sistemul RIC.

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

Disponibilitatea se asigură prin funcţionarea continuă a tuturor componentelor sistemului RIC. Diverse aplicaţii au nevoie de nivele diferite de disponibilitate în funcţie de impactul sau daunele produse ca urmare a nefuncţionării corespunzătoare a sistemului RIC.

Politica de securitate are ca scop, de asemenea, stabilirea cadrului necesar pentru elaborarea regulamentelor şi procedurilor de securitate. Acestea sunt obligatorii pentru toţi utilizatorii sistemului RIC.

1.3 Definiţii folosite în politica de securitate şi regulamentul de utilizare

Resurse Informatice şi de Comunicaţii (RIC):
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: mainframe-uri, servere, calculatoare personale, calculatoare-agendă (notebook-uri), calculatoare de buzunar, asistent digital personal (*Personal Digital Assistant* - PDA), sisteme de procesare distribuită, echipament 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 creea, colecta, înregistra, procesa, stoca, primi, afişa şi transmite informaţia.

Responsabilul cu protecţia datelor (DPO): Este persoana de contact intern şi extern a Achizitorului /CREART pentru orice problemă în legătură cu securitatea RIC.
Responsabilul cu protecţia datelor are următoarele sarcini:
(a) informarea şi consilierea institutiei precum şi a angajaţilor care se ocupă de prelucrare, cu privire la obligaţiile care le revin în temeiul Regulamentului general privind protecţia datelor şi al altor dispoziţii de drept al Uniunii sau drept intern referitoare la protecţia datelor;
(b) monitorizarea respectării Regulamentului general privind protecţia datelor, a altor dispoziţii de drept al Uniunii sau de drept intern referitoare la protecţia datelor şi a politicilor societăţii sau ale persoanei împuternicite în ceea ce priveşte protecţia datelor cu caracter personal, inclusiv alocarea responsabilităţilor şi acţiunile de sensibilizare şi de formare a personalului implicat în operaţiunile de prelucrare, precum şi auditurile aferente;
(c) furnizarea de consiliere la cerere în ceea ce priveşte evaluarea impactului asupra protecţiei datelor şi monitorizarea funcţionării acesteia;
(d) cooperarea cu autoritatea de supraveghere;
(e) asumarea rolului de punct de contact pentru autoritatea de supraveghere privind aspectele legate de prelucrare precum şi, dacă este cazul, consultarea cu privire la orice altă chestiune.

Utilizator: O persoană, o aplicaţie automatizată sau proces utilizator autorizat de către CREART, în conformitate cu procedurile şi regulamentele în vigoare, să folosească RIC.

Abuz de privilegii: Orice acţiune întreprinsă în mod voit de un utilizator, care vine în contradicţie cu regulamentele Achizitorului 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.

Operator economic : Persoană fizică/juridică care furnizeaza bunuri, presteaza servicii, executa lucrari in folosul Achizitorului /CREART în baza unui contract .

Internet: Sistem global care interconectează calculatoare şi reţele de calculatoare. Acestea sunt deţinute de mai multe organizaţii, agenţii guvernamentale, societăţi, instituţii academice.

Intranet: Reţea privată destinată comunicaţiilor şi partajării informaţiilor, care, ca şi reţeaua Internet, foloseşte suita de protocoale TCP/IP, însă este accesibilă doar utilizatorilor autorizaţi din cadrul unei organizaţii (instituţii). În mod obişnuit, reţeaua Intranet a unei organizaţii este protejată printr-un sistem de protecţie (firewall).

Virus: Un program care se auto-ataşează la un fişier executabil sau la o aplicaţie vulnerabilă şi care generează efecte de la cele deranjante până la cele distructive. Un virus se execută în momentul în care este

accesat un fişier infectat. Un virus de macro infectează codul executabil încapsulat în pachetul de programe Microsoft Office (Word, Excel, PowerPoint) sau alte programe care permit utilizatorului să genereze macro-uri.

Worm: Un program care se auto-copiază în oricare altă parte a unui sistem informatic. Aceste copii pot fi create pe acelaşi calculator sau pot fi trimise către alte calculatoare prin intermediul reţelei. Prima utilizare a termenului descria un program care s-a multiplicat într-o reţea de calculatoare, folosind resursele sau calculatoarele neutilizate din reţea pentru a distribui aceste copii. Unii dintre aceşti „viermi" reprezintă o ameninţare la adresa securităţii datorită faptului că folosesc reţeaua pentru a se împrăştia, împotriva voinţei proprietarilor de sisteme de calcul, cauzând astfel nefuncţionarea sau funcţionarea defectuoasă a reţelei. Un worm este asemănător unui virus prin faptul că se auto-copiază, diferenţa constând în faptul că un worm nu are nevoie să se ataşeze la anumite fişiere pentru a se multiplica.

Cal troian: de obicei un virus sau un worm – care este ascuns sub forma unui program atractiv sau inofensiv, cum ar fi un joc, sau program de grafică (o felicitare în format electronic, un program tip screen-saver). Victimele pot primi un astfel de cal troian prin email sau pe o dischetă, adeseori de la o altă victimă necunoscută sau pot fi încurajate să descarce un fişier de pe o pagină Web sau un forum.

Incident de Securitate: În termeni informatici este definit ca un eveniment prin care se încearcă sau se realizează accesul la un sistem informatic, un atac asupra integrităţii şi/sau confidenţialităţii informaţiei de pe un sistem informatic automatizat. Aceasta include examinarea sau navigarea neautorizată, întreruperea sau anularea unui serviciu, date alterate sau distruse, prelucrarea (procesarea), stocarea sau extragerea informaţiilor, modificarea informaţiilor sistemului referitoare la caracteristicile componentelor hardware, firmware sau software cu sau fără ştiinţa sau intenţia utilizatorului.

Reţea locală (LAN): O reţea de comunicaţii de date ce este distribuită pe o zonă restrânsă (de regulă la nivelul unui grup de lucru). Reţeaua locală oferă comunicaţii între calculatoare şi periferice la o viteză de transfer mare şi cu puţine erori.

Server: Un program de calculator care oferă servicii altor programe aflate pe acelaşi calculator sau pe calculatoare diferite. Un calculator care rulează un program tip server este denumit în mod frecvent server, cu toate că pe acelaşi calculator mai pot rula şi alte programe de tip client sau server.

Gazdă (Host): Un sistem care oferă servicii pentru un anumit număr de utilizatori.

Copii de Siguranţă (backup): Copii ale fişierelor şi aplicaţiilor făcute pentru a evita pierderea datelor şi pentru a permite recuperarea în cazul unor evenimente care pot conduce la pierderi de date.

Firewall: Un mecanism de control al accesului care acţionează ca o barieră între două sau mai multe segmente ale unei reţele de calculatoare sau ale unei arhitecturi de tip client/server, folosit pentru a proteja reţelele interne sau segmente ale acestora împotriva utilizatorilor sau proceselor neautorizate.
Atac informaţional: O încercare de a trece peste măsurile şi controalele de securitate fizice sau informatice care protejează un sistem din cadrul sistemului de RIC. Atacatorul poate altera informaţiile, poate acorda sau refuza accesul la ele. Succesul unui eventual atac depinde de gradul de vulnerabilitate al sistemului în particular şi de eficacitatea contramăsurilor aplicate.

Protecţie informaţională: Acţiuni întreprinse în vederea afectării informaţiilor şi sistemelor informatice ostile, în timp ce protejează informaţiile şi sistemele informatice proprii.

Procedura - reprezintă modalitatea specifică de desfăşurare a unei activităţi sau a unui proces.

1.4 Clasificarea Informaţiilor

Clasificarea informaţiilor este necesară pentru a permite atât alocarea resurselor necesare protejării acestora cât şi pentru a determina pierderile potenţiale ca urmare a modificărilor, pierderii/distrugerii sau divulgării acestora.

Pentru a asigura securitatea şi integritatea informaţiilor, acestea se împart în trei categorii principale:

- Publice;
- Secrete;
- Confidenţiale.

DPO şi conducerea instituţiei răspund de evaluarea periodică a schemei de clasificare a informaţiilor. Toate informaţiile din CREART trebuie să se regăsească în una din următoarele categorii:

1. ***Publice.*** Acestea sunt informaţiile accesibile oricărui utilizator din interiorul sau exteriorul sediului Achizitorului/CREART. Divulgarea, utilizarea neautorizată sau distrugerea acestora nu produce efecte asupra Achizitorului/CREART sau aceste efecte sunt nesemnificative. Utilizatorii care furnizează aceste informaţii sunt responsabili de asigurarea integrităţii şi disponibilităţii acestora în raport cu cerinţele CREART.
2. ***Secrete.*** În această categorie se includ informaţiile pe care Achizitorul/CREART trebuie să le protejeze conform legislaţiei în vigoare. Aceste date trebuie distruse dacă au fost făcute publice. Aceste date vor fi copiate şi distribuite în cadrul CREART doar utilizatorilor autorizaţi. Distribuirea acestor informaţii de către utilizatorii autorizaţi trebuie să se facă pe baza unei clauze de confidenţialitate.
3. ***Confidenţiale.*** În această categorie se includ toate informaţiile care datorită valorii naturii lor nu trebuie făcute publice. Divulgarea, utilizarea sau distrugerea acestor date poate intra sub incidenţa Codului Civil, Penal sau legislaţiei în vigoare. Accesul la aceste informaţii va fi restricţionat. Datele strict secrete nu pot fi copiate, distribuite sau şterse fără acordul scris al conducerii Achizitorului /CREART.

1.5 Confidenţialitate

1. Fişierele electronice create, trimise, primite sau stocate folosind sistemul RIC propriu, administrate sau în custodia şi sub controlul Achizitorului/CREART nu au caracter personal şi pot fi accesate oricând de către angajaţii autorizaţi (specialistul IT/administrator reţea) fără înştiinţarea utilizatorului.
2. În scopul administrării RIC şi pentru asigurarea securităţii RIC personalul autorizat poate revizui sau utiliza orice informaţie stocată sau transportată prin sistemele RIC în conformitate cu legile în vigoare. În aceleaşi scopuri, este posibilă monitorizarea activităţii utilizatorilor.
3. Utilizatorii trebuie să raporteze orice slăbiciune în sistemul de securitate al calculatoarelor din cadrul CREART, orice incident de posibilă întrebuinţare greşită sau încălcare a acestui regulament (prin contactarea DPO).
4. Un mare număr de utilizatori, pot accesa diverse informaţii din sistemul de comunicaţii al CREART. În aceste condiţii este obligatorie păstrarea confidenţialităţii acestor informaţiilor transmise din exteriorul RIC şi a informaţiilor obţinute din interior.
5. Utilizatorii nu trebuie să încerce să acceseze informaţii sau programe de pe sistemele CREART pentru care nu au autorizaţie sau consimţământ explicit.
6. Nici un utilizator al sistemului RIC ale Achizitorului/CREART nu poate divulga informaţiile la care are acces sau la care a avut acces ca urmare a unei vulnerabilităţi a sistemului RIC. Această

regulă se extinde şi după ce utilizatorul a încheiat relaţiile cu CREART, conform angajamentelor personale sau contractelor de munca semnate, existente in cadrul Serviciului Resurse Umane.

7. Confidenţialitatea informaţiilor transmise prin intermediul resurselor de comunicaţii ale terţilor nu poate fi asigurată. Pentru aceste situaţii, confidenţialitatea şi integritatea informaţiilor se poate asigura folosind tehnici de criptare. Utilizatorii sunt obligaţi să se asigure că toate informaţiile confidenţiale ale Achizitorului /CREART se transmit în aşa fel încât să se asigure confidenţialitatea şi integritatea acestora.

Cap. II. Regulamentele de Utilizare a Resurselor Informatice şi de Comunicaţii (RIC)

Introducere

Regulamentele de Utilizare a 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 CREART. Acestea au ca scop principal protejarea utilizatorilor, colaboratorilor împotriva atacurilor de orice tip (cu sau fără intenţie). De asemenea acestea au ca scop protejarea imaginii instituţiei şi a investiţiilor acesteia pentru dezvoltarea sistemul informatic şi de comunicaţii.

Scopul acestor regulamente este acela de a asigura:

- Stabilirea unor reguli corecte, echitabile şi eficiente pentru folosirea resurselor informatice şi de comunicaţii;
- Protejarea imaginii CREART;
- Protejarea investiţiilor CREART pentru dezvoltarea sistemului informatic şi de comunicaţii propriu;
- Protejarea proprietăţii intelectuale şi a tuturor informaţiilor stocate şi transportate folosind Resursele Informatice şi de Comunicaţii ale utilizatorilor autorizaţi: membrii conducerii, personal contractual, colaboratori etc.
- Educarea utilizatorilor resurselor informatice şi de comunicaţii în ceea ce priveşte responsabilităţile asociate cu utilizarea acestora;
- Compatibilitate cu regulamentele, statutul şi atribuţiile stabilite pentru administrarea resurselor informatice şi de comunicaţii

Regulamentele de utilizare a resurselor informatice şi de comunicaţii ale Achizitorului/ CREART se aplică nediscriminatoriu tuturor persoanelor cărora li s-a permis accesul la acesta.

Regulamentele şi procedurile de lucru sunt elaborate de DPO şi supuse spre aprobare conducerii.

Prevederile Politicii de Securitate şi Procedurile de Lucru aprobate vor fi aplicate tuturor entităţilor şi utilizatorilor după cum urmează:

- Angajaţii cu contract de muncă pe perioadă determinată sau nedeterminată care au acces la sistemul informaţional şi de comunicaţii;
- Colaboratorii Achizitorului /CREART care au acces la sistemul RIC;
- Operatori economici care au acces la sistemul RIC;
- Alte persoane, entităţi sau organizaţii care au acces la sistemul RIC conform prevederilor legale.

Modificarea regulamentului şi/sau a procedurilor generale de lucru se va face ori de câte ori este nevoie, iar aprobarea modificărilor se va face de către conducere la propunerea DPO.

Procedurile Generale de Lucru fac parte integrantă din prezentul regulament.

2.1 Regulament de utilizare a RIC

1. Utilizarea sistemului RIC se efectueaza numai în interes de serviciu.
2. Utilizatorii trebuie să anunţe DPO în cazul în care se observă orice problemă/breşă în sistemul de securitate a RIC din cadrul CREART cât şi orice posibilă întrebuinţare greşită sau încălcare a regulamentelor în vigoare.
3. Utilizatorii, prin acţiunile lor, nu trebuie să încerce să compromită protecţia sistemelor informatice şi de comunicaţii şi nu trebuie să desfăşoare, deliberat sau accidental, acţiuni care pot afecta confidenţialitatea, integritatea şi disponibilitatea informaţiilor de orice tip în cadrul sistemului RIC al Achizitorului/CREART.
4. Utilizatorii nu trebuie să încerce să obţină acces la date sau programe din RIC pentru care nu au autorizaţie sau consimţământ explicit.
5. Utilizatorii nu trebuie să divulge sau să înstrăineze nume de cont-uri, parole, Numere de Identificare Personală (PIN-uri), dispozitive pentru autentificare (ex.: Smartcard) sau orice dispozitive şi/sau informaţii similare utilizate în scopuri de autorizare şi identificare.
6. Utilizatorii nu trebuie să copieze neautorizat sau să distribuie materiale protejate prin legile privind proprietatea intelectuală (copyright).
7. Utilizatorii nu trebuie să utilizeze programe de tip shareware sau freeware, fără aprobare, cu excepţia cazului în care acestea se găsesc pe lista programelor standard folosite în cadrul Achizitorului/CREART. Această listă va fi întocmită în funcţie de necesităţile departamentelor.
8. Utilizatorii nu trebuie:
   - să degradeze performanţele RIC;
   - să obţină alte resurse în afara celor alocate;
   - să nu ia în considerare măsurile de securitate impuse prin regulamente;
   - să exploateze defectuos componentele RIC;
   - să utilizeze orice suport de stocare a informaţiei din exteriorul instituţiei fără acordul explicit al DPO;
9. Utilizatorii nu trebuie să descarce, instaleze şi să ruleze programe de securitate sau utilitare care expun sau exploatează vulnerabilităţi ale securităţii RIC. De exemplu, utilizatorii Achizitorului /CREART nu trebuie să ruleze programe de decriptare a parolelor, de captură de trafic, de scanări ale reţelei sau orice alt program nepermis de regulamente.
10. RIC ale Achizitorului /CREART nu trebuiesc folosite pentru beneficiul personal.
11. Utilizatorii nu trebuie să acceseze, să creeze, să stocheze sau să transmită materiale pe care CREART le poate considera ofensive, indecente sau obscene (altele decât cele pentru care aprobarea explicită a conducerii instituţiei).
12. Accesul la reţeaua Internet prin intermediul RIC se supune aceloraşi regulamente care se aplică utilizării din interiorul instituţici;
13. Angajaţii nu trebuie să permită membrilor familiei sau altor persoane străine neautorizate, care nu au aprobare explicită din partea DPO sau a conducerii instituţiei accesul la RIC ale CREART.
14. Utilizatorii care au acces la sistemul RIC al CREART au obligaţia de a purta acte şi/sau legitimaţii/ecusoane care să ateste calitatea de utilizator autorizat în spaţiile CREART.
15. Utilizatorii nu trebuie să se angajeze în acţiuni împotriva scopurilor CREART folosind RIC.
16. În cazul demisiei/plecării definitive din instituţie a unui utilizator acest lucru va fi comunicat de către Compartimentului Resurse Umane din cadrul instituţiei. DPO va dispune la stergerea conturilor şi parolelor utilizatorului respectiv, iar accesul utilizatorului la RIC va fi interzis.
17. Este interzisă utilizarea RIC de către persoane neautorizate.

2.2. Utilizarea ocazională a RIC în scopuri personale

În aceste situaţii se aplică următoarele restricţii:

1. Utilizarea personală ocazională a serviciilor de poştă electronică, acces internet, telefoane, fax-uri, imprimante, copiatoare, etc. este restricţionată la utilizatorii autorizaţi şi nu poate fi extinsă la membrii familiilor sau alte persoane.

2. Utilizarea ocazională a RIC nu trebuie să aibă drept rezultate costuri directe pentru Achizitor/CREART.
3. Utilizarea ocazională a RIC nu trebuie să afecteze activitatea normală a angajaţilor.
4. Nu este permisă trimiterea sau recepţionarea documentelor sau fişierelor care pot cauza acţiuni legale împotriva Achizitorului /CREART sau prejudicierea, indiferent de formă, a intereselor Instituţiei.
5. Stocarea mesajelor de email, a mesajelor de voce, a documentelor şi fişierelor personale din cadrul RIC trebuie să fie nominală.
6. Toate mesajele, fişierele şi documentele – incluzând mesajele personale, fişierele şi documentele – localizate în cadrul RIC sunt proprietatea Instituţiei şi pot fi subiectul unor cereri de verificare/inspectare/accesare de către DPO sau Directorul general conform regulamentelor.

2.3. Accesul Administrativ

1. Utilizatorii trebuie să cunoască şi să accepte toate regulamentele privind securitatea RIC înainte de a li se permite accesul la un cont.
2. Utilizatorii care au conturi de acces administrativ trebuie sa aibă instrucţiuni de administrare, documentare, instruire şi autorizare a conturilor. Aceste instrucţiuni se vor elabora de către fiecare Compartiment şi vor fi incluse în fişa postului.
3. Utilizatorii cu drepturi administrative sau speciale de acces nu trebuie să folosească în mod abuziv aceste drepturi şi trebuie să facă investigaţii numai sub îndrumarea DPO sau Responsabilului IT.
4. 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.
5. Accesul administrativ trebuie să se conformeze **Politicii de parolare**
6. Parola pentru un cont cu acces privilegiat nu va fi utilizată de mai multe persoane decât cu acordul scris al DPO şi trebuie să fie schimbată atunci când o persoana care utilizează acest cont îşi schimbă locul de muncă din cadrul compartimentului sau a instituţiei, sau în cazul unei modificări a listei de personal ale terţilor în contractele cu Achizitorul/ CREART
7. Trebuie să existe o procedură prin care o altă persoană, în afară de administrator, să poată avea acces la contul administratorului în caz de forţa majoră. Această procedură va fi elaborată de către DPO şi comunicată Responsabilului IT aflat în cauză.
8. Unele conturi sunt necesare pentru audit (verificare, control) intern sau extern, pentru dezvoltare sau instalare de software sau alte operaţiuni definite. Acestea trebuie să îndeplinească următoarele condiţii:
    - trebuie să fie autorizate;
    - trebuiesc create cu dată de expirare specifică;
    - contul va fi şters atunci când nu mai este necesar.

2.4. Accesul Fizic

1. Accesul fizic la toate încăperile în care sunt instalate RIC trebuie să fie documentat şi monitorizat.
2. Toate încăperile în care sunt instalate RIC trebuie să fie protejate fizic, în funcţie de importanţa acestora şi tipul datelor vehiculate sau stocate.
3. Pentru fiecare încăpere în care sunt instalate echipamente ale sistemului RIC se aprobă accesul doar pentru personalul care răspunde de buna funcţionare a echipamentelor din încăperea respectivă şi, dacă este cazul, părţilor contractante, ale căror obligaţii contractuale implică acces fizic.
4. Personalul care are drepturi de acces trebuie să deţină legitimaţie de serviciu şi acte de identitate care să-i ateste calitatea.
5. Nu este permis transferul dreptului de acces indiferent de motiv.

6. Accesul publicului, vizitatorilor, sau a persoanelor străine în cadrul instituţiei se efectueaza doar pe baza actului de identitate. Vizitatorii/persoanele străine trebuie să fie însoţiţi în zonele cu acces restricţionat.
7. Pentru fiecare spaţiu în care sunt instalate RIC se va păstra o evidenţă a accesului pentru verificări de rutină în situaţii critice.

2.5. Conectarea la Sistemul Resurselor Informatice şi de Comunicaţii

1. Utilizatorilor le este permis să utilizeze numai parametrii pentru conectare la reţea specificaţi de către administratorul de reţea.
2. Pentru fiecare sistem conectat trebuie să existe o persoană care să răspundă de acesta, numele şi datele de identificare ale acesteia se vor comunica către DPO.
3. Conectarea sistemelor de calcul care nu sunt proprietatea Achizitorului /CREART se face numai cu aprobarea în scris din partea conducerii instituţiei.
4. Accesul de la distanţă la reţeaua Achizitorului/CREART se va realiza numai prin echipamente aprobate, sau prin intermediul unui Furnizor de Servicii Internet (Internet Service Provider (ISP)) agreat de către CREART şi folosind protocoale aprobate de către DPO.
5. Utilizatorii RIC din interiorul sediului Achizitorului/CREART nu se pot conecta la altă reţea.
6. 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. Autorizarea tuturor conexiunilor se face la propunerea Departamentelor de către Compartimentul de Informatică.
7. Utilizatorii nu trebuie să instaleze echipamente hardware sau programe care furnizează servicii de reţea fără aprobarea Compartimentului de Informatică.
8. Sistemele computerizate din afara Instituţiei care necesită conectare la reţea trebuie să se conformeze cu standardele reţelei interne ale CREART.
9. Utilizatorii nu au dreptul să descarce din Internet, să instaleze sau să ruleze programe de securitate sau de altă natură care pot dezvălui slăbiciuni în securitatea unui sistem. De exemplu, utilizatorii CREART nu au dreptul să ruleze programe de spargere a parolei, sustragere de pachete, scanare a porturilor, în timp ce sunt conectaţi la reţeaua Instituţiei.
10. Utilizatorii nu au dreptul să modifice, reconfigureze, instaleze, dezinstaleze echipamente de reţea, cabluri, prize de conexiuni.
11. Serviciul de nume şi administrarea adreselor IP sunt deservite exclusiv de către Compartimentul de Informatică.
12. Serviciile de interconectare a reţelei CREART cu alte reţele sunt realizate exclusiv de către Compartimentul de Informatică.
13. Nu este permisă instalarea şi/sau modificarea echipamentelor utilizate pentru conectare la reţea (inclusiv plăci de reţea) fără aprobarea Compartimentul de Informatică. Tipul şi modelul plăcilor de reţea şi tuturor echipamentelor care se pot conecta în reţea trebuie să fie aprobate de către Compartimentul de Informatică.

2.6. Configurarea Parametrilor de Acces la Reţea

1. Infrastructura de comunicaţii, reţeaua de comunicaţii digitale, a Achizitorului /CREART este administrată de către o societate externalizata care este responsabila cu întreţinerea acesteia.
2. Pentru a furniza o infrastructură de comunicaţii unitară cu posibilităţi de modernizare toate componentele acesteia sunt instalate de către de către un furnizor avizat explicit.
3. Toate echipamentele, fără excepţie, conectate la reţeaua de comunicaţii trebuie configurate conform specificaţiilor.
4. Orice dispozitiv care se va conecta la reţeaua Achizitorului/CREART, trebuie să fie însoţit de o aprobare de tip (producător, model etc.).