Nr. 2483/12.06.2024

# INVITAȚIE DE PARTICIPARE LA PROCEDURA „LICITAȚIE"

Informatică Feroviară S.A., cu sediul în Str Gării de Nord nr. 1, Sector 1, București, Cod Poștal 010855, Telefon 0212232778, înregistrată la Registrul Comerțului cu nr. J40/10636/2002, C.I.F. RO14966210, vă invită să depuneți oferta pentru atribuirea contractului "Servicii subscripție Antivirus +EDR".

| Nr. crt. | Denumire produs/ serviciu/ lucrare | Cod CPV |
|---|---|---|
| 1 | Servicii subscripție Antivirus + EDR | 72910000-2 |

1. **Sursa de finanțare a contractului** : surse proprii
2. **Procedura aplicată** pentru atribuirea contractului "Servicii subscripție Antivirus +EDR" este **licitație.**
3. **Criteriul de atribuire:** prețul cel mai scăzut
4. **Limba de redactare a ofertei:** română;
5. **Perioada de valabilitate a ofertei:** 30 de zile calendaristice de la termenul limită de depunere a ofertei;
6. **Ofertantul este obligat să depună ofertă:**
   - 6.1 **Pentru toate reperele solicitate în caietul de sarcini** [X]
   - 6.2 **Pentru reperele din portofoliul de produse, servicii sau lucrări ale ofertantului** [ ]

   **NU SE ACCEPTA oferte parțiale sau alternative.**
7. **Documentele de calificare solicitate și care însoțesc obligatoriu oferta sunt:**
   (se selectează din lista de mai jos, în funcție de complexitatea achiziției)
   - ✓ Copie certificat de înregistrare al societății la Registrul Comerțului,
   - ✓ Certificat constatator emis de ONRC din care să rezulte că obiectul de activitate al ofertantului include activități ce fac obiectul achiziției și faptul ca ofertantul nu este în procedura de faliment. Data emiterii acestuia trebuie să fie cu cel mult 30 de zile inainte de data limită de depunere a ofertelor **(se solicită numai ofertantului declarat câștigător).**
   - ✓ Certificat de atestare fiscală privind impozitele și taxele locale **(se solicită numai ofertantului declarat câștigător)**

- ✓ Certificat de atestare fiscală privind obligațiile la Bugetul de stat (**se solicită numai ofertantului declarat câștigător**)
- ✓ Cazier judiciar societate (**se solicită numai ofertantului declarat câștigător**)
- ✓ Împuternicire prin care operatorul economic desemnează o persoană să îl reprezinte în relația cu Informatică Feroviară S.A. **(Formularul F-10-029-12)**
- ✓ Declarație privind situatia personala a ofertantului, îndeplinirea obligațiilor exigibile de plată către bugetul de stat și bugetul local, indeplinirea criteriilor de selectie **(Formularul F-10-029-13)**
- ✓ Informații generale **(Formularul F-10-029-14)**
- ✓ Experiența similară. Se vor prezenta documente care să ateste implementarea a minim 2(două) soluții similare pentru organizații cu minim 1.000 terminale și minim 1.500 cutii poștale. **(Formularul F-10-029-15)**
- ✓ Declarație privind conflictul de interese **(Formularul F-10-029-17)**
- ✓ Declarație de acceptare a condițiilor contractuale **(Formularul F-10-029-25)**
- ✓ **Alte documente de calificare solicitate prin caietul de sarcini (certificate, atestate, standarde, etc...)**

**Documente de selecție:**

- ✓ **Oferta tehnică**
- ✓ **Formularul de ofertă financiară (Formularul F-10-029-18)**

*Datele cu caracter personal furnizate direct sau prin documente solicitate sunt utilizate numai în scopul derulării procedurii de achiziție. Protecția datelor cu caracter personal vehiculate în scopul parcurgerii etapelor privind achiziția de bunuri servicii sau lucrări este asigurată conform legislației în vigoare.*

*Informatică Feroviară S.A. asigură măsuri tehnice și organizatorice pentru ca prelucrarea datelor cu caracter personal să se facă cu respectarea principiilor și drepturilor persoanelor vizate, prevăzute de Regulamentul nr. 679/2016*

*Prin furnizarea documentelor solicitate ofertantul își exprimă acordul pentru prelucrarea datelor furnizare, în scopul derulării procedurii de achiziție.*

**Ofertantul va depune documentele solicitate în original sau copie semnată și ștampilată cu mențiunea conform cu originalul de către reprezentantul legal/împuternicit.**

8. **Modul de prezentare a propunerii tehnice:**

Prin propunerea tehnică depusă, ofertantul are obligaţia de a face dovada conformităţii produselor / serviciilor ce urmează a fi livrate / prestate, cu cerinţele prevăzute în Caietul de sarcini nr. 1958/08.05.2024 (Revizia I).

**9. Modul de prezentare a propunerii financiare:**

Oferta Financiară va include categoriile de produse/servicii solicitate, preţul unitar pe produs şi valoarea totală, pe modelul prezentat în tabelul de mai jos:

| Denumire serviciu | | | Cant. | Preţ unitar (lei fără TVA) | Valoare An 1 (lei fără TVA) | Valoare An 2 (lei fără TVA) | Valoare An 3 (lei fără TVA) | Valoare totalaă contract (lei fără TVA) |
|---|---|---|---|---|---|---|---|---|
| **1. Servicii de subscripţie antivirus + EDR** | | | 1 | | | | | |
| 1.1 | **1.1.a Terminale din care** | | **7.900** | | | | | |
| | 1.1.a1 | - Servere | 500 | | | | | |
| | 1.1.a2 | - Staţii de lucru | 7.400 | | | | | |
| | **1.1.b Cutii poştale** | | **9.000** | | | | | |
| | **Total valoare pct 1.1 (lei fără TVA)** | | | | | | | |
| 1.2 | Servicii auxiliare de asistenţă configurare şi instruire | | 1 | | | | | |
| **Valoare totală (lei fără TVA)** | | | | | | | | |

Oferta financiară depusă este fermă şi conformă cu cerinţele caietului de sarcini.

Preţul va fi exprimat în lei, fără TVA şi este ferm pe perioada de valabilitate a contractului.

Preţul va include toate cheltuielile şi comisioanele care vor fi angajate de către furnizor/prestator.

Compararea preţurilor prevăzute în propunerile financiare ale ofertanţilor se realizează la valoarea totală, fără TVA.

Evaluarea ofertelor se realizează prin compararea preţurilor fiecărei oferte admisibile în parte şi prin întocmirea clasamentului, în ordine crescătoare a preţurilor respective, pe baza căruia se stabileşte oferta câştigătoare.

**Evaluarea ofertelor se va face pentru valoarea totală a ofertei depuse** [X]

**Evaluarea ofertelor se va face pentru fiecare reper ofertat** [ ]

**10. Aplicarea criteriului de atribuire:**

**1. La valoare totală per ofertă** [X]

**2. La valoare totală per reper** [ ]

**11. Moneda în care se transmite oferta de preț lei.**

**12. Modul de transmitere al ofertei.**

Ofertele vor fi depuse de către operatorii economici în plicuri sigilate, într-un exemplar original, marcat clar „original" și o copie, cu marcarea „copie". În cazul unor discrepanțe între acestea, prioritate va avea originalul. Fiecare plic original și copie va conține la rândul său cate un plic sigilat marcat cu „Documente de calificare", „Oferta tehnică" și „Oferta financiară".

**Ofertele operatorilor economici vor fi depuse la secretariatul Informatică Feroviară S.A. până la data 21.06.2024 ora 10:00**

Solicitările de clarificări vor putea fi transmise până la data de 17.06.2024

Raspunsurile la solicitări vor fi transmise până cel târziu la data de 19.06.2024

**13. Modalitati/termene de plată**

Plata se va efectua anual, prin virament bancar, în termen de 30 de zile de la emiterea facturii. Factura va fi emisă după cum urmează:

Pentru primul an contractual, factura va fi emisă după semnarea de ambele părţi a procesului verbal de recepție și acceptanță care confirmă că:

-pe site-ul producătorului, în contul alocat beneficiarului, este stipulată perioada de valabilitate a subscriptiilor pentru fiecare tip de terminal prevăzut în caietul de sarcini nr.1958/08.05.2024 (Revizia I).

-serviciile auxiliare au fost prestate în conformitate cu prevederile caietul de sarcini nr. 1958/08.05.2024 (Revizia I).

Pentru anul 2 şi 3 contractual, factura va fi emisă după semnarea de ambele părţi a procesului verbal de acceptanţă care confirmă că în consola de administrare a soluţiei, pe site-ul producătorului este actualizată perioada de valabilitate a subscripţiilor şi numărului de terminale pentru ca e se acorda subscripţia.

14. **Termenul de implementare al contractului:** 60 de zile de la semnarea contractului.

**Durata contractului este de 3 ani.**

15. **Câştigătorul** va fi ofertantul care îndeplineşte toate cerinţele solicitate şi este clasat pe primul loc conform criteriului de atribuire stabilit în prezenta procedură.

16. **Garanţia de bună execuţie:** Furnizorul se obligă să constituie garanţia de bună execuţie, prin virament bancar, printr-un instrument de garantare emis în condiţiile legii de o societate bancară sau de o societate de asigurări sau prin depunere la casieria Informatică Feroviară S.A. (sumele care nu depăşesc 5.000 lei) care devine anexă la contract valabilă pe toată perioada de valabilitate a contractului, în cuantum de 5% din valoarea fără TVA a contractului. Aceasta va trebui să fie prezentată achizitorului în termen de 5 zile lucrătoare de la data semnării contractului.

Se solicită [X] Nu se solicită [ ]

Restituirea garanţiei de bună execuţie se va face în baza cererii de restituire respectiv **Formularul F-10-029-19**

17. **Respingerea ofertelor/anularea procedurii**

**Ofertele pot fi:**

1. **corespunzătoare** - este oferta care îndeplineşte toate cerinţele din documentaţia de achiziţie (atât cerinţele cât şi specificaţiile tehnice). **Aceasta este considerată ofertă admisibilă.**

2. **necorespunzătoare** - este oferta care nu îndeplineşte toate cerinţele din documentaţia de achiziţie (fie cerinţele, fie specificaţiile tehnice). **Acestea pot fi inacceptabile sau neconforme.**

**Oferta este considerată inacceptabilă în următoarele situaţii:**

a) a fost depusă de un ofertant care nu îndeplineşte una sau mai multe dintre criteriile de calificare stabilite în documentaţia de achiziţie;

b) preţul, fără TVA, inclus în propunerea financiară depăşeşte valoarea resurselor financiare alocate în BVC şi PAA şi nu există posibilitatea disponibilizării de fonduri

suplimentare pentru îndeplinirea contractului de achiziție respectiv. În conformitate cu procedura proprie de achiziție valoarea estimată nu se comunică operatorilor economici;

c) are o valoare neobișnuit de mică iar justificările primite nu sunt concludente;

d) oferta este depusă după data și ora limită stabilită pentru depunerea ofertelor;

e) ofertantul refuză să prelungească perioada de valabilitate a ofertei;

f) în cazul în care unei oferte îi lipsește una din cele două componente (propunerea financiară sau propunerea tehnică).

g) ofertantul depune mai mult de o ofertă financiară

**Oferta este considerată neconformă în următoarele situații:**

a) nu satisface în mod corespunzător cerințele caietului de sarcini;

b) conține propuneri de modificare a clauzelor contractuale pe care le-a stabilit achizitorul în cadrul documentației de achiziție, care sunt în mod evident dezavantajoase pentru acesta din urmă, iar ofertantul, deși a fost informat cu privire la respectiva situație, nu acceptă renunțarea la clauzele respective.

c) conține în cadrul propunerii financiare prețuri care nu sunt rezultatul liberei concurențe și care nu pot fi justificate;

d) propunerea financiară nu este corelată cu elementele propunerii tehnice ceea ce ar putea conduce la executarea defectuoasă a contractului, sau constituie o abatere de la legislația incidentă.

**Anularea procedurii se poate face în următoarele cazuri:**

Anularea procedurii se poate face în orice etapă a procedurii, până la semnarea contractului.

Informatică Feroviară S.A. nu va fi responsabilă pentru orice fel de daune, inclusiv fără limitare, daune pentru pierderea profitului, în orice mod legate de anularea unei proceduri de achiziție.

## 18. Modalități de contestare a deciziei de atribuire a contractului de achiziție și de soluționare a contestației

Contestațiile privind Comunicarea rezultatului procedurii de achiziție pot fi depuse în termen de 2 zile lucrătoare de la data primirii comunicării. Contestațiile pot fi depuse în scris la Secretariatul Informatică Feroviară sau transmise prin email la adresa office@infofer.ro

Contestațiile vor fi analizate și soluționate de către Informatică Feroviară S.A. într-un termen de maxim 2 zile lucrătoare de la data înregistrarii lor. Termenul de răspuns se poate prelungi cu maxim 15 zile lucrătoare dacă achiziția este complexă.

## 19. Precizări finale

Adunarea Generală a Acționarilor a Informatică Feroviară S.A. a acordat Consiliului de Administrație prin Hotarârea nr. 6/26.05.2005, competență să aprobe încheierea sau

rezilierea contractelor a căror valoare este peste suma de 1.000.000 lei fără TVA. Până la această sumă, competența de aprobare revine Directorului General.

Ca urmare a celor prezentate mai sus, contractele a căror valoare depășesc suma de 1.000.000 lei fără TVA se vor încheia numai după obținerea aprobării Consiliului de Administrație.

**Avizat,**
**Director Departament SIIT**
**Adrian AMBROSĂ**

**Aprobat,**
**Director Economic**
**Liliana CEPLEU**

SOCIETATEA COMERCIALĂ 2 INFORMATICĂ FEROVIARĂ S.A BUCUREȘTI

Nr inregistrare 1958/08.05.2024 Data
Revizia I

APROBAT,
DDI / M AIF
Adrian AMBROSĂ

# CAIET DE SARCINI

I. **Achizitor:** INFORMATICĂ FEROVIARĂ S.A. cu sediul în București, Str. Gării de Nord nr. 1, sector 1, cod poștal 010855.

II. **Obiectul achiziției:** (denumirea contractului de achiziție) Soluție extinsă de protecție anti-malware pentru stații de lucru, servere și e-mail, furnizată ca "Servicii subscripție Antivirus + EDR"

III. **Denumire produs/serviciu/lucrare / cod CPV:**

| | Denumire produs/ serviciu/ lucrare | Cod CPV |
|---|---|---|
| 1 | Servicii subscripție Antivirus + EDR | 72910000-2 |

## IV. Cerințe pentru completarea ofertei tehnice

*Propunerea tehnică va fi depusă cu respectarea cerințelor prevăzute în Caietul de sarcini.*

### 1. Cerințe generale

În cadrul serviciilor subscribție Antivirus + EDR se va furniza o soluție extinsă de protecție anti-malware pentru stații de lucru, servere și e-mail pe bază de abonament.

Scopul soluției este protejarea de amenințări de securitate cibernetică la nivelul stațiilor de lucru, a serverelor și a fluxului de poștă electronică. Soluția trebuie să asigure monitorizare comportamentală, a proceselor sistemului de operare, acțiunilor utilizatorilor și a traficului de rețea pentru identificarea atacurilor multi-vector sofisticate de tip ransomware sau APT. protejarea fluxului de poștă electronică trebuie să se asigure multinivel, atât pe serverele de poștă electronică cât și pe terminale inspectarea fișierelor, a metadatelor și a conținutului.

Soluția solicitată va fi formată din următoarele componente:

A. Soluție de protecție anti-malware la nivel de stații de lucru și servere
B. Soluție de detecție și răspuns la nivel de stații de lucru și servere (EDR)
C. Soluție de protecție anti-malware, anti-phishing și anti-spam pentru serverele de e-mail.

Soluția trebuie să protejeze un număr de inițial de 7.900 de terminale, dintre care 500 de servere (fizice sau virtuale) și 7.400 stații de lucru și un număr inițial de 9.000 de cutii poștale. Pe durata derulării contractului, cantitățile se pot suplimenta cu maxim 25% cu păstrarea prețului unitar.

**Pentru toate aceste componente se solicită servicii de suport tehnic și mentenanță pe toată durata de valabilitate a contractului.**

Soluția propusă va fi integrată la nivel de management (consolă de management, un singur punct de vizualizare și administrare) cel puțin pentru componentele (A) și (B).

Componentele soluției trebuie să utilizeze o bază de date comună de Indicatori de Compromis (IOCs) pe baza cărora să se poată identifica și bloca amenințări la nivelul fiecărei componente.

*Funcționalități de management centralizat:*

Pentru administrare soluția trebuie să ofere o platformă centralizată cu acces tip HTTPS, cu autentificare multi-factor, pe bază de roluri cu drepturi de administrare sau vizualizare pe zone definite de terminale, utilizatori și grupuri Active Directory, astfel încât administratorilor soluției să le fie alocate drepturi conform responsabilităților avute.

Platforma trebuie să ofere următoarele funcții raportare:

- Șabloane predefinite și posibilitatea de a crea rapoarte noi.
- Opțiunea configurării de ecrane tip tablou de bord pentru informare, alertare și prioritizarea acțiunilor operaționale
- Ecrane predefinite, specifice evenimentelor legate de vulnerabilități, din care să se poată urmări cel puțin: listele de alerte critice, evoluția riscurilor, top aplicații vulnerabile detectate, top evenimente prevenite, stare actualizare agenți.

*În ofertă vor fi identificate distinct serviciile auxiliare (Cap. 3) pentru instruirea a minim 16 administratori de soluție, servicii de asistență tehnică pentru implmeentare și configurare și servicii de suport tehnic pentru atacuri de tip 0-day sau amenințări care nu au fost detectate de produs.*
*Serviciile de suport (Cap.4) sunt incluse în serviciul principal pe bază de abonament pe perioada contractului.*

## 2. Cerințe specifice

## A. Soluția de protecție la nivel de stații de lucru și servere

2.A.1. Principalele categorii de funcționalități ale componentei stații de lucru și servere

- Anti-malware
- Protecție împotriva amenințărilor avansate
- Analiză comportamentală pentru atacuri sofisticate (anti-exploit, 0-day)
- Firewall local
- Control al perifericelor la nivelul stațiilor de lucru
- Controlul vulnerabilităților și al actualizărilor la nivelul sistemului de operare (opțional)
- Control al aplicațiilor care pot fi utilizate pe terminal
- Control al site-urilor Web accesate
- Protecție împotriva ransomware

### 2.A.2 Funcționalități anti-malware

Soluția va folosi o bază de date reputațională pentru prefiltrare, care să includă liste cu fișiere cunoscute și liste de prevalență a fișierelor. Actualizările legate de bazele de date reputaționale trebuie să fie disponibile într-un singur punct de distribuție, folosind o componentă proprie a soluției.

La nivelul următor agentul de securitate va oferi o componentă de analiză comportamentală la nivel de fișiere, cu următoarele funcționalități:

- Identificarea comportamentelor rău-intenționate și detecția comportamentelor anormale ale aplicațiilor care ar putea determina o amenințare sau un atac.
- Protecție împotriva script-urilor și rootkit-urilor.
- Protecție împotriva atacurilor cu cod injectat.
- Protecție împotriva rulării exploit-urilor în browser.
- Protecție a fișierelor, serviciilor și a cheilor de registri Windows.

Agentul de securitate al soluției va oferi metode de scanare la nivel de memorie, în vederea detectării amenințărilor malware fără fișier, care rulează doar în memorie.

Soluția permite administratorului sa stabilească acțiunea luata de produsul Anti-malware la detectarea unei amenințări noi. Astfel administratorul va putea alege intre următoarele acțiuni:

- Acțiune implicită pentru fișiere infectate: interzice accesul / dezinfectează / ștergere / mută fișierele în carantină / nicio acțiune
- Acțiune alternativă pentru fișierele infectate: interzice accesul / dezinfectează / ștergere / mută fișierele în carantină
- Acțiune implicită pentru fișierele suspecte: interzice accesul / ștergere / mută fișierele în carantină / nicio acțiune
- Acțiune alternativă pentru fișierele suspecte: interzice accesul / ștergere / mută fișierele în carantină.

**2.A.3. Protecție împotriva amenințărilor avansate**
Acest modul monitorizează procesele care rulează și evaluează comportamente suspecte, de exemplu camuflarea tipului de proces, execuția de cod în spațiul de memorie al altui proces cu privilegii superioare, replicare, creare de fișiere, ascundere de aplicațiile de monitorizare procese. Fiecare comportament suspect ridică nivelul de alarmă până la atingerea nivelului de notificare și acțiune.

**2.A.4 Analiză comportamentală pentru atacuri sofisticate (anti-exploit, 0-day)**
Pentru o mai bună protecție a stațiilor și serverelor, soluția include protecție împotriva atacurilor zero-day de tip exploit avansate (atacuri direcționate) bazată pe tehnologii de învățare automată (machine learning).

Soluția de protecție la nivel de endpoint trebuie să includă mecanisme de tip Machine Learning, acționând atât în perioada de dinaintea execuției, cât și după momentul execuției. Pentru a scădea rezultatele fals-pozitive, soluția trebuie să ofere funcționalități de prefiltrare în procesul de detecție.

Soluția trebuie să ofere un mecanism de protecție pentru malware-ul de tip zero-day prin Monitorizarea Comportamentală (Behavior Monitoring) și configurarea evenimentelor de acțiune pentru cel puțin următoarele:

- Duplicarea fișierelor de sistem;
- Modificarea fișierului host;
- Modificarea politicilor de securitate;
- Injectarea în librăriile de programe (DLL injection);
- Modificări aduse prin rularea terminalelor de tip Shell;
- Creare de servicii noi;
- Modificarea fișierelor sistem;
- Modificarea politicii de firewall;
- Modificare în sistem a proceselor;
- Adăugare sau modificare procesului de startup;

Acest modul avansat de securitate va proteja împotriva: atacurilor direcționate (Targeted Attack - APT), fișierelor suspecte și traficului la nivel de rețea suspect, exploit-urilor, ransomware și grayware. Fiecărui tip de amenințare menționat, i se vor putea stabili, independent, un nivel de protecție dorit: permisiv, normal, agresiv.

Modulul avansat de securitate are posibilitatea de a raporta, bloca accesul, dezinfecta, șterge sau muta în carantină pentru fiecare din categoriile descrise. Astfel, administratorul va putea decide daca dorește întâi monitorizare sau dorește și blocarea amenințărilor. Aceste acțiuni menționate, vor putea fi stabilite independent, pentru fișiere sau pentru traficul din rețea, cu posibilitatea extinderii nivelului de raportare pentru a include nivelurile superioare (vor putea fi raportate amenințările care ar fi fost detectate dacă nivelul de protecție era stabilit mai agresiv).

**2.A.5 Firewall local**

- Posibilitatea de a configura reguli de firewall pentru aplicații sau conectivitate.
- Posibilitatea de a seta diferite profiluri de rețea ((Home/Office, Trusted, Public, Untrusted sau Let the Windows decide)
- Abilitatea de a crea reguli personalizate bazate pe aplicație și/sau conexiune

- Modulul va detecta atacurile din rețea ce au ca obiectiv compromiterea terminalului: scanări de porturi și atacuri de tip forță-brută pentru mișcare laterală, atacuri asupra serviciilor web de tip injecție SQL, atacuri prin trafic de rețea ex. botnets.
- Modulul de firewall este o sursă de telemetrie / date despre atac pentru componenta EDR.
- Detecția și blocarea tentativelor de conectare către resurse cunoscute ca fiind centre de comandă și control (C&C).

### 2. A.6 Control al perifericelor

Clientul local, în conjuncție cu componenta de management centralizat, permite:

- Prevenția de potențiale infecții cu malware sau scurgerea accidentală sau intenționată de date prin atașarea de dispozitive externe. Sunt gestionabile toate device-urile de stocare/comunicații de sistem (Medii de stocare portabile respectiv conexiuni Bluetooth, IEEE 1284.4, IEEE 1394, Modem, porturi COM/LPT, adaptor de rețea Ethernet sau Wireless).
- Modulul permite capturarea unor informații specifice legate de dispozitivele externe cum ar fi: nume, class ID, momentul în timp când a fost conectat.
- Modulul va permite configurarea de reguli prin care se vor defini permisiunile pentru dispozitivele conectate la mașină client cum ar fi: permis/blocat/custom respectiv poate limita accesul dispozitivelor externe la „read only" sau limita doar accesul la porturile USB ale endpoint-ului permițând orice alt tip de dispozitiv ce nu folosește acest tip de port/interfață.
- Modulul va permite configurarea de excluderi pentru diferite tipuri de dispozitive pentru care s-au configurat reguli pe baza a /Device/Hardware ID.
- Modulul poate „descoperi" noi dispozitive și raporta prezența acestora în consola de management.

### 2.A.7 Control al aplicațiilor

Pentru o mai bună inventariere și administrare, soluția va include o secțiune în consola de administrare unde se vor regăsi toate aplicațiile descoperite în rețea după: nume, versiune, găsit pe.

Pentru prevenirea infectării stațiilor și serverelor dar și pentru a permite aplicațiilor descoperite în rețea să se poată actualiza, soluția permite definirea unor programe de actualizare (Updater) care vor fi lăsate să actualizeze diferite aplicații instalate pe stații sau servere.

Acest modul poate funcționa în modul Whitelisting (prin care se blochează accesul la toate aplicațiile cu excepția celor menționate în lista alba) sau Blacklisting (prin care se blochează doar accesul la aplicațiile menționate în lista neagră).

### 2.A.8 Control al accesului la site-uri Web

Clientul local, în conjuncție cu componenta de management centralizat, permite:

- Blocare pagini de internet după tip de conținut sau categorii prestabilite.
- Adăugarea de liste de acces sau blocare particulare la nivelul companiei.
- Agentul de securitate va oferi un mecanism de scanare reputațională pentru resursele web accesate inclusiv HTTPS.
- Soluția va permite detecția și blocarea tentativelor de conectare către resurse cunoscute ca fiind centre de comandă și control (C&C)

### 2.A.9 Gestiunea vulnerabilităților și a actualizărilor

- Soluția trebuie să ofere posibilitatea de a vedea toate patch-urile care lipsesc din mediu. Aceste informații ar trebui să fie agregate într-un inventar de patch-uri.
    - Soluția va oferi vizibilitate a punctelor finale instalate sau lipsește un patch specific.
    - Soluția va oferi informații și motive în cazul în care un patch nu se instalează
    - Soluția va oferi utilizatorului posibilitatea de a instala rapid patch-urile lipsă
    - Administratorul ar trebui să poată opri sau suspenda aplicarea uneia sau a mai multor actualizări.
- Soluția va oferi raportarea patch-urilor lipsă din perspectiva punctului final (patch-uri instalate / lipsă pe fiecare punct final)
- Capacitatea de a funcționa în modul automat sau manual
    - Programarea scanărilor pentru patch-ul lipsă
    - Programarea instalării automate separată pe baza categoriei de patch-uri (securitate / non-securitate)
    - Posibilitatea de a amâna repornirea stațiilor de lucru, dacă instalarea patch-ului o solicită.
    - Posibilitatea de descoperire și instalare a patch-urilor la cerere (manual)
- Soluția va oferi posibilitatea de stocare a patch-urilor pe o mașină special desemnată (caching server), în acest fel patch-urile vor fi descărcate de pe internet numai de către unele puncte finale atribuite.

### 2. A.10 Protecție împotriva ransomware

Pentru o mai buna protecție a stațiilor și serverelor, soluția include un vaccin anti-ransomware. Acest vaccin asigură protecția împotriva tuturor amenințărilor cunoscute de tip ransomware, prin imunizarea stațiilor și serverelor, chiar dacă sunt infectate și prin blocarea procesului de criptare.

Vaccinul anti-ransomware primește actualizări de la producător, odată cu actualizarea semnăturilor produsului anti-malware.

### 2.A.11 Soluție de verificare tip Sandbox

Pentru a oferi un nivel adițional de protecție a stațiilor și serverelor, soluția include un sandbox în cloud-ul public al producătorului acesteia / opțional on-premise.

Modulul de Sandbox include doua variante de analiză: doar monitorizare sau blocare. În modul monitorizare utilizatorul va putea accesa fișierul dorit, pe când în modul blocare, utilizatorului i se va bloca rularea fișierului până când Sandbox-ul din cloud-ul producătorului va da verdictul.

Modulul de Sandbox include doua tipuri de acțiuni remediere: implicită și de siguranță. Pentru acțiunea implicită se va putea stabili: doar raportare, dezinfecție, ștergere și carantinare. Pentru acțiunea de siguranță se va putea stabili: ștergere sau carantinare.

Modulul de Sandbox folosește configurații vulnerabile (minim 2 generații de sistem de operare anterior, sisteme neactualizate) pentru a identifica fișiere cu comportament malițios, a crea semnături și IOCs și a le transmite spre celelalte module ale soluției.

Modulul de Sandbox poate suporta „detonarea" următoarelor tipuri de fișiere: Batch, CHM, DLL, EML, Flash SWF, HTML, HTML/script, HTML (Unicode), JAR (archive), JS, LNK, MHTML (doc), MHTML (ppt), MHTML (xls), Microsoft Excel, Microsoft PowerPoint, Microsoft Word,

MZ/PE files (executabile), PDF, PEF (executabile), PIF (executabile), RTF, SCR, URL (binare), VBE, VBS, WSF, WSH, WSH-VBS, XHTML.

Fișierele menționate anterior, vor putea fi detectate corect chiar dacă sunt incluse în arhive de tipul: : 7z, ACE, ALZip, ARJ, BZip2, cpio, GZip, LHA, Linux TAR, LZMA Compressed Archive, MS Cabinet, MSI, PKZIP, RAR, Unix Z, ZIP, ZIP (multivolume), ZOO, XZ.

**2.A.12 Cerințe de sistem de operare:**

Soluția trebuie să poată asigura un nivel de protecție maximă pentru terminale și servere cu sisteme de operare Microsoft Windows, Microsoft Windows Server, macOS și Linux în suport producător.

Producătorul va oferi versiuni anterioare (mai vechi) ale clientului anti-malware și anti-virus pentru sisteme de operare ce nu se mai află în suport producător, minim două generații în urmă, ca opțiune de downgrade parțial.

**2.A.13 Alte cerințe:**

- Agentul trebuie să dispună de metode de protecție împotriva modificărilor neautorizate de politici sau dezactivării de funcționalități, inclusiv împotriva dezactivării întregului produs.
- Pentru a limita impactul operațional și încărcarea sistemelor, soluția trebuie să optimizeze resursele CPU alocate motorului anti-malware atât în timp real, cât și pentru scanările programate.
- Soluția trebuie să permită excluderea directoarelor unde sunt instalate soluții terțe de securitate ex.: Endpoint DLP.
- Soluția va include funcționalități de server de update on premise (ca rol distinct sau ca rol adițional al unui terminal) pentru actualizările de versiune, semnături și IOCs ale soluției de protecție la nivel endpoint.

## 2.B. Soluție avansată de detecție și răspuns:

**2.B.1. Principalele capabilități și funcționalități ale componentei de detecție avansată:**

Scopul componentei este detectarea, corelarea și răspunsul la evenimente de tip EDR („endpoint detection and response") pentru a identifica amenințări avansate sau atacuri în curs de desfășurare.

Acest modul cuprinde un senzor de colectare de date și evenimente despre hardware și software aferent fiecărei stații de lucru aducând informații detaliate referitoare la incidentele detectate, o hartă detaliată a acestora precum și acțiuni de remediere automate și integrare cu modulele de Sandbox și modulul avansat de analiză de securitate.

Colectare de telemetrie extinsă la nivel de stație de lucru prin agentul comun cu soluția de protecție la nivel de endpoint instalat și stocarea telemetriei extinse trimise de agent într-o bază de date de securitate. Pe baza acestor date componenta EDR are capacitatea de a evalua activitatea tipică a unui endpoint din perspectiva securității acestuia conform tehnicilor de atac MITRE („baselining") și poate raporta orice deviație de la acest comportament sub forma unui incident.

Include reguli de detecție predefinite iar pe baza acestora să coreleze și să alerteze incidentele identificate la nivelul stațiilor de lucru. Regulile sunt configurabile pe criteriile proces, fișier, regiștri, conexiuni de rețea.

Componenta EDR permite filtrarea incidentelor din interfața grafică în funcție de intervalul de timp, pe baza unui scor de încredere („confidence score"), indicatori de atac, tehnici de atac (ATT&CK) respectiv sistem de operare afectat cât și după IP, nume fișier, nume stație. Componenta EDR permite vizualizarea detaliată a incidentelor incluzând detalii specifice fiecărui nod afectat.

**2.B.2. Cerințe funcționale:**

- Platforma ofertată de tip EDR trebuie să poată corela date din multiple elemente de protecție cum ar fi email, stații de lucru, servere sau telemetrie de rețea (minim pe baza clientului anti-malware sau prin senzor de rețea adițional).
- Platforma EDR trebuie să pună la dispoziția operatorului de investigație cibernetică o hartă grafică a atacului și a resurselor implicate (utilizator, resurse de calcul, IP uri, URL, fișiere, chei regiștri, procese etc.) și maparea evenimentelor în matricea MITRE ATT&CK.
- Soluția EDR trebuie poată reconstrui firul execuției la nivel de host, astfel încât analistul să poată urmări lanțul logic de execuție și relaționare a evenimentelor până la cauza inițială a atacului (root cause analysis), se așteaptă folosirea în cadrul investigației de diverse obiecte relevante de forensics: fișiere, procese, domenii, adrese IP și porturi, servicii, regiștri Windows.
- Modulul de investigații al incidentelor trebuie să permită căutarea după indicatori de compromis și alți identificatori, de exemplu nume fișier, cale fișier, suma de control a fișierului (File Hash), cont de utilizator, adresa IP, înregistrare DNS, cheie / nume / date de regiștri Windows, comenzi de sistem.
- Soluția trebuie să permită crearea de excepții de detecție și răspuns.
- Se pot excepta fișiere non-malițioase de la acțiunea de investigare sau se pot genera/adăuga un set de fișiere malițioase într-o listă neagră pentru a preveni mișcarea laterală a fișierelor/proceselor malițioase.
- Opțiuni de intervenție ale operatorului:
    - Izolarea, respectiv repunerea în funcțiune a stației de lucru: stația de lucru suspectă să nu mai poată comunica cu nici o altă resursă, în afară de platforma de securitate pentru analiză suplimentară.
    - Colectarea fișierelor suspicioase pentru analiză suplimentară.
    - Pornirea unei scanări anti-malware
    - Adăugarea de obiecte suspicioase în lista Indicatorilor de Compromis centralizată din pagina de incident.

## 2.C. Protecție și securitate pentru servere mail Microsoft Exchange

2.C.1 Compatibilitate: Microsoft Exchange 2019 cu rol de Edge Transport sau Mailbox

**2.C.2 Funcționalități:**

*Protecție anti-malware, anti-spam, anti-phishing, anti-spyware prin integrare cu serverul Microsoft Exchange*

- Scanarea atașamentelor și a conținutului mesajelor în timp real, fără a afecta vizibil performanța serverului de mail.
- Scanarea la cerere a bazelor de date Exchange.
- Actualizarea anti-malware trebuie să poată fi făcută automat la un interval de maxim 1 oră, precum și la cerere.
- Protecție pe bază de semnături și scanare euristică comportamentală, prin simularea unui calculator virtual în interiorul căruia sunt rulate și analizate

aplicații cu potențial periculos, pentru a proteja sistemul de virușii necunoscuți prin detectarea codurilor periculoase a căror semnătură nu a fost lansata încă.
- Detecția amenințărilor cunoscute, incluzând: amenințări zero-day, detecție true file type, detecție a emulării de scripturi, analiza pentru gestiunea fișierelor deformate, detecția și analiza exploit-urilor din documente, atacuri cu embedded exploit code.
- Blocarea URL-urilor specificate de către administratorii soluției.
- Soluția include opțiunea de gestionare a carantinei la nivel centralizat de către administratorii soluției.

*Anti-spam*

- Modulul anti spam va trebui să includă un filtru URL cu o bază de adrese URL cunoscute și/sau filtre RBL a fi folosite în mesaje spam, precum și un filtru de caractere pentru detectarea automată a mesajelor scrise cu caractere chirilice sau asiatice.
- Produsul va trebui să ofere un serviciu/filtru online pentru îmbunătățirea protecției împotriva valurilor de spam nou apărute.

*Mecanisme/metode de eliminare a obiectelor infectate din mesaje, înainte de transmiterea acestora către utilizatori.*

Facilitatea de configurare și aplicare a cel puțin următoarelor acțiuni post-detecție: eliminarea atașamentelor infectate din mesaj, ștergerea mesajului, blocarea mesajului și trimiterea în carantină, aplicarea unor etichete (texte definite de administrator) în mesaj, transmiterea directă fără modificare.

*Cerințe specifice pentru mediu sandbox ale soluției de detecție și răspuns la nivel de email*

- Suport granular la nivel de politică pentru a trimite anumite tipuri de fișiere (ex.: exe, pdf, docx, etc.) către soluția de Sandbox astfel încât se pot excepta spre trimiterea în sandbox pentru anumiți destinatari sau grupuri de destinatari.
- Suport pentru analiza a cel puțin următoarelor tipuri de fișiere:
    - Office, cu sau fără macro (ex: doc, docx, rtf, xls, xlsx, ppt, pptx).
    - Executabile și script-uri (ex: exe, bat, cmd, class, ps1, vbs, vbe, wsf).
    - Fișiere ce pot conține link-uri și script-uri - PDF, Flash, multimedia, Java, resurse, etc. (ex: pdf, swf, flv, xml, jar, js, htm, html, svg, chm).
    - Arhive, inclusiv arhive multi-nivel (ex: zip, rar, p7, tar, tgz, gz, bz2).
- Suport pentru analiza URL-urilor.

*Management*

- Produsul va oferi posibilitatea de a defini politici de filtrare anti malware, anti spam, a conținutului sau atașamentelor pentru diferite grupuri sau utilizatori.
- Actualizarea produsului va fi configurabilă și se va putea realiza de pe internet, direct sau printr-un proxy, sau din cadrul rețelei de pe un server de actualizare propriu.
- Produsul va trebui sa ofere statistici atât referitoare la scanarea antivirus cât și la scanarea anti spam.
- Produsul se poate integra în cadrul consolei de management unitar al soluției antivirus. Pentru ușurința accesului la setările produsului din diferite medii de operare, produsul va avea consolă de administrare web.
-

*Secțiunea Alerte, rapoarte și log-uri ale soluției de detecție și răspuns la nivel de email*

- Generare de rapoarte în mod programat sau la cerere, incluzând cel puțin următoarele facilități:
    - generare rapoarte.
    - transmisie rapoarte prin e-mail către anumiți destinatari sau liste de destinatari.
    - descărcare rapoarte direct din consola de management.
- Vizualizarea log-urilor de sistem în consola de management, incluzând facilitatea de filtrare după cel puțin următoarele elemente: tipul evenimentului sau al log-ului, dată/oră sau interval de timp. De asemenea, soluția trebuie să permită exportul log-urilor, integral sau particularizat în urma aplicării filtrelor.
- Log-urile operaționale ale soluției trebuie să cuprindă evenimente de la cel puțin următoarele componente:
    - jurnale ale detecțiilor.
    - jurnale de transport.
    - jurnale asociate acțiunilor realizate de utilizatori la nivelul URL-urilor rescrise.
- Transmisia către sisteme externe de tip syslog sau SIEM a cel puțin următoarelor tipuri de evenimente generate de către soluție:
    - evenimente de sistem (alerte / notificări).
    - evenimente legate de detecții.
    - evenimente de transport al emailurilor.
- Log-urile trimise către sisteme externe de tip syslog sau SIEM trebuie să fie structurate cel puțin în următorul format standard: Common Event Format (CEF).
- Un sistem de alerte și notificări, care în baza unor reguli predefinite să poată trimite notificări sub forma de e-mail către liste de contacte configurabile. Activarea și dezactivarea notificărilor, precum și frecvența trimiterii acestora trebuie să poată fi configurate din interfața de management.
- Soluția permite configurarea conținutului notificărilor transmise.

**3. Servicii auxiliare:**

- Instruirea unui număr de minim 16 administratori de soluție privind arhitectura generală a produsului oferit și a soluțiilor tehnice implementate, a instalării, configurării și administrării întregii soluții.
- Servicii de asistență tehnică în implementarea soluției / on-boarding - supervizarea instalării și configurării unui eșantion proporțional de stații de lucru cu diverse sisteme de operare, gazde pentru mediul de virtualizare, servere de aplicație, servere de poștă electronică. Acest eșantion va reprezenta minim 10% din totalul end-point-urilor din organizație.

  Configurarea se va face în conformitate cu *bestpractice*-urile producătorului.

**4. Servicii de suport pentru toate componentele soluției pe perioada contractului:**

- Suport tehnic în condiții de SLA în cazul unor atacuri de tip 0-day, amenințări care nu au fost detectate de produs sau *false-positive*:
    - În cazul în care sunt afectate servicii esențiale sau un număr mai mare de 5% din numărul total de terminale:
        - timp de răspuns la apel: 1oră,

- timp de identificare: 5 ore
- timp de remediere provizorie sau blocare a amenințării: 12 ore

- În cazul în care nu sunt afectate servicii esențiale sau un număr mai mare de 5% de terminale:
  - timp de răspuns la apel: 12 ore,
  - timp de identificare: 24 ore
  - timp de remediere provizorie sau blocare a amenințării: 48 ore

## V. Standarde solicitate:

ISO 9001 și ISO 27001 pentru furnizorul soluției.

## VI. Certificări solicitate:

Se va prezenta un document eliberat de producătorul soluției care să certifice autorizarea ofertantului pentru a furniza către Informatica Feroviară:

- Soluție;
- servicii de asistență în implementare;
- servicii de suport tehnic și mentenanță pe durata contractului.

## VII. Calificări solicitate:

Pentru ducerea la îndeplinire a cerințelor din Caietul de sarcini ofertantul va prezenta dovezi de certificare de la producătorul soluției privind competențele de implementare și suport pentru minim 2 specialiști.

## VIII. Experiență similară:

Se vor prezenta documente care să ateste implementarea a minim două soluții similare pentru organizații cu minim 1.000 de terminale și minim 1.500 de cutii poștale.

Numărul minim de terminale și cutii poștale se poate echivala cu implementări de volum mai mic la organizații cu cerințe de securitate crescute (instituții financiare, furnizori de servicii esențiale sau critice).

## IX. Livrarea și recepția:

Furnizorul va oferi pachetele de instalare pentru terminale și accesul pentru administratorii din partea Beneficiarului în platforma de management. Numărul total de obiecte protejate de soluție va fi vizibil în consola de management sau într-un fișier sau document ce atestă dreptul de utilizare în cantitățile solicitate.

Serviciile în integralitate, atât soluția de protecție pe bază de abonament cât și serviciile auxiliare, se consideră recepționate după semnarea de ambele părți a procesului verbal de recepție și acceptanță care confirmă că soluția de protecție funcționează și este în conformitate cu cerințele prezentului caiet de sarcini, în termen de maxim 60 de zile de la semnarea contractului.

**X. Ambalarea și transportul:**

Nu se aplică.

**XI. Termenul de garanție:**

Nu se aplică.

**XII. Termenul de implementare al contractului:** *60 de zile de la semnarea contractului*

**XIII. Alte condiții minimale obligatorii pe care trebuie să le îndeplinească oferta:**

Ofertanții vor respecta prevederile legii 354/2022.

**XIV. Precizări finale.**

Ofertantul declarat câștigător are obligația de a nu transfera parțial sau în total obligațiile sale asumate, fără să obțină în prealabil acordul scris al achizitorului.

Întocmit,
Cobianu Cezar, consultant în informatică

**Draft Contract de prestări servicii**

**Nr.....**

Preambul:

Având în vedere Raportul de evaluare nr. .....pentru atribuirea contractului de achiziție " **Servicii subscripție Antivirus +EDR"**, prin care a fost desemnată câștigătoare oferta firmei ....., s-a încheiat prezentul contract între:

**Societatea** ..... în calitate de **PRESTATOR**

Și

**INFORMATICĂ FEROVIARĂ S.A.**, cu sediul în București, Str. Gării de Nord, nr. 1, sector 1, cod 010855, Telefon: 021 2232778, Fax: 021 2232779, înmatriculată la Registrul Comerțului sub nr. J40/10636/2002, cod de înregistrare fiscală nr. RO14966210, având contul: RO23BTRL04501202339214XX deschis la Banca Transilvania, Agenția Gara de Nord, reprezentată prin: RADU Alexandru - Director General și Liliana CEPLEU, Director Economic, în calitate de **ACHIZITOR.**

**I. OBIECTUL CONTRACTULUI.**

**ART.1** (1) Prezentul contract are ca obiect **Soluție extinsă de protecție anti-malware pentru stații de lucru, servere și e-mail, furnizată ca "Servicii subscripție Antivirus + EDR"** pentru echipamentele menționate în **Anexa 1** la contract, Caietului de sarcini nr. **1958/08.05.2024 Revizia I -Anexa nr.2** la contract și Oferta tehnică-nr.....**Anexa 3** la contract:

| Nr.crt. | Denumire serviciu | Cantitate |
|---|---|---|
| 1. | 1. Servicii de subscripție antivirus + EDR | 1 |
| 1.1 | 1.1 a Terminale din care | 7900 |
| | 1.1 a 1 Servere | 500 |
| | 1.1 a 2 Stații de lucru | 7400 |
| | 1.1b Cutii poștale | 9000 |
| 1.2. | Servicii auxiliare de asistență configurare și instruire | 1 |

(2) In conformitate cu prevederile Caietului de sarcini 1958/08.05.2024 Revizia I pe parcursul derulării contractului cantitățile se pot suplimenta cu maxim 25% cu păstrarea prețului unitar.

## II. DURATA ȘI TERMENUL DE IMPLEMENTARE A CONTRACTULUI.

**ART.2** (1) Contractul intră în vigoare la data constituirii garanției de bună execuție conform Cap.VIII din contract, are o durată de 3 ani și se poate prelungi prin act adițional.

(2) Conform prevederilor Caietului de sarcini nr. 1958/08.05.2024 Revizia I, furnizorul va oferi pachetele de instalare pentru terminale și accesul pentru administratorii din partea Beneficiarului în platforma de management. Numărul total de obiecte protejate de soluție va fi vizibil în consola de management sau într-un fișier sau document ce atestă dreptul de utilizare în cantitățile solicitate.

Serviciile în integralitate, atât soluția de protecție pe bază de abonament cât și serviciile auxiliare, se consideră recepționate după semnarea de ambele părți a procesului verbal de recepție și acceptanță care confirmă că soluția de protecție funcționează și este în conformitate cu cerințele prezentului caiet de sarcini, în termen de maxim 60 de zile de la semnarea contractului.

(3) Conform prevederilor Caietului de sarcini nr. 1958/08.05.2024 Revizia I, termenul de implementare al contractului este de 60 de zile de la semnarea contractului.

## III. VALOAREA CONTRACTULUI.

**ART.3** Valoarea contractului este de .....**lei** la care se adaugă TVA conform **Anexei nr.1** care face parte integrantă din prezentul contract.

**ART.4** Prețul serviciilor este ferm și cuprinde toate cheltuielile și comisioanele ce vor fi angajate de prestator în scopul realizării contractului.

## IV. MODALITĂȚI DE PLATĂ.

**ART.5** (1) Plata se va efectua anual, prin virament bancar, în termen de 30 de zile de la emiterea facturii.

**ART.6** Factura va fi emisă după cum urmează:

a) Pentru primul an contractual, factura va fi emisă după semnarea de ambele părți a procesului verbal de recepție și acceptanță care confirmă că:

-pe site-ul producătorului, în contul alocat beneficiarului, este stipulată perioada de valabilitate a subscriptiilor pentru fiecare tip de terminal prevăzut în caietul de sarcini nr.1958/08.05.2024 Revizia I.

-serviciile auxiliare au fost prestate în conformitate cu prevederile caietul de sarcini nr. 1958/08.05.2024 Revizia I.

b) Pentru anul 2 și 3 contractual, factura va fi emisă după semnarea de ambele părți a procesului verbal de acceptanță care confirmă că în consola de administrare a soluției, pe site-ul producătorului este actualizată perioada de valabilitate a subscripțiilor și numărului de terminale pentru care se acorda subscripția.

**V. OBLIGAŢIILE PRESTATORULUI.**

**ART.7** Să dețină toate avizele prevăzute de legislația în vigoare pentru prestarea de servicii care fac obiectul prezentului contract.

**ART.8** Să constituie garanția de bună execuție conform Cap.VIII.

**ART.9** Prestatorul se obligă să presteze serviciile care fac obiectul contractului conform clauzelor prezentului contract și prevederilor Caietului de sarcini nr. 1958/08.05.2024 Revizia I.

**ART.10** Prestatorul este pe deplin responsabil pentru execuția și securitarea serviciilor care fac obiectul contractului și garantează prestarea acestora cu profesionalismul și promptitudinea cuvenite angajamentului asumat.

**ART.11**(1) Prestatorul se obligă să garanteze calitatea serviciilor executate în baza prezentului contract pe toata perioada de executare a contractului și să asigure suportul tehnic aferent.

(2) Serviciile vor fi prestate cu specialişti certificaţi conform prevederilor Caietului de sarcini nr. 1958/08.05.2024 Revizia I.

(3) Prestatorul se obligă să acorde Suport tehnic în condiții de SLA în cazul unor atacuri de tip 0-day, amenințări care nu au fost detectate de produs sau *false-positive*:

- În cazul în care sunt afectate servicii esențiale sau un număr mai mare de 5% din numărul total de terminale:
  - timp de răspuns la apel: 1oră,
  - timp de identificare: 5 ore
  - timp de remediere provizorie sau blocare a amenințării: 12 ore
- În cazul în care nu sunt afectate servicii esențiale sau un număr mai mare de 5% de terminale:
  - timp de răspuns la apel: 12 ore,
  - timp de identificare: 24 ore
  - timp de remediere provizorie sau blocare a amenințării: 48 ore

**ART.12** Prestatorul se obligă să-şi instruiască personalul propriu şi să respecte obligaţiile legale referitoare la condiţiile de muncă, protecţia muncii, apărare împotriva incendiilor şi protecţia mediului şi poartă întreaga răspundere fată de accidentele de muncă suferite de personalul său. Eventualele accidente de muncă suferite de personalul Prestatorului, ivite pe parcursul derulării prezentului contract se înregistrează la Prestator.

**ART.13** Prestatorul va păstra confidenţialitatea tuturor documentelor, informaţiilor şi datelor furnizate de Achizitor pentru îndeplinirea prevederilor contractului şi nu le va transmite către terţi fără acordul scris al Achizitorului.

## VI. OBLIGAŢIILE ACHIZITORULUI.

**ART.14** Achizitorul are obligaţia de a achita preţul contractului la valoarea şi termenele stabilite.

**ART.15** Să păstreze confidenţialitatea documentelor, informaţiilor şi datelor puse la dispoziţie de către Prestator pentru îndeplinirea obiectului contratului şi să nu le transmită către terţi, fără acordul acestuia.

## VII. RĂSPUNDEREA CONTRACTUALĂ.

**ART.16** În cazul în care Prestatorul nu reuşeşte să-şi îndeplinească, îndeplineşte cu întârziere sau necorespunzător obligaţiile asumate până la scadenţă, atunci va plati Achizitorului penalităţi în cuantum de 0,04% pe ziua de întârziere din valoarea contractului, începând cu prima zi lucrătoare după data scadenţei până la îndeplinirea efectivă a obligaţiilor.

**ART.17** În cazul în care Achizitorul nu îşi onorează obligaţiile până la terminarea perioadei convenite la art.5, atunci acestuia îi revine obligaţia de a plăti, ca penalităţi, o sumă echivalentă cu o cotă de 0,04% pe ziua de întârziere din plata neefectuată, începând cu prima zi lucrătoare dupa data scadenţei, până la data efectuării plăţii.

**ART.18** Neîndeplinirea şi/sau îndeplinirea necorespunzătoare a obligaţiilor asumate de către părţi prin prezentul contract atrage răspunderea părţii aflate în culpă. În cazul angajării răspunderii contractuale, potrivit prevederilor prezentului articol, partea aflată în culpă este obligată la acoperirea integrală a prejudiciului.

## VIII. GARANŢIA DE BUNĂ EXECUŢIE

**ART.19** Prestatorul are obligaţia de a constitui garanţia de bună execuţie a contractului de prestări servicii în scopul asigurării achizitorului cu privire la îndeplinirea integrală a obligaţiilor contractuale, în termen de 5 zile lucrătoare de la data semnării contractului de ambele părţi.

**ART.20** Garanţia de bună execuţie se constituie într-un cuantum de **5 %** din valoarea totală a contractului fără TVA .... lei în favoarea Informatică Feroviară S.A., prin virament bancar , printr-un instrument de garantare emis în condiţiile legii de o societate bancară sau de o societate de asigurări sau prin depunere la casieria Informatică Feroviară S.A. (sumele care nu depăşesc 5.000 lei) care devine anexă la contract valabilă pe toată perioada de valabilitate a contractului.

**ART.21** Termenul de valabilitate al garanţiei de bună execuţie trebuie să fie mai mare cu minimum 14 zile faţă de termenul de valabilitate a contractului.

**ART.22** (1) Achizitorul are dreptul de a emite pretenţii asupra garanţiei de bună execuţie, oricând pe parcursul îndeplinirii contractului, în limita prejudiciului creat, în cazul în care Prestatorul nu îşi îndeplineşte din culpa sa obligaţiile asumate prin contract.

(2) Anterior emiterii unei pretenţii asupra garanţiei de bună execuţie Achizitorul are obligaţia de a notifica pretenţia Prestatorului, precizând obligaţiile care nu au fost respectate, precum şi modul de calcul al prejudiciului. În situaţia executării garanţiei de bună execuţie, parţial sau total, Prestatorul are obligaţia de a reîntregi garanţia în cauză raportat la restul rămas de executat.

(3) Achizitorul are obligaţia de a elibera/restitui garanţia de bună execuţie Prestatorului în cel mult 14 zile de la data îndeplinirii de către Prestator a obligaţiilor contractuale, dacă nu a ridicat până la acea dată pretenţii asupra ei.

## IX. CLAUZE DE CONFIDENŢIALITATE

**ART.23** Părțile se obligă să păstreze confidențialitatea oricăror date și informații, indiferent de suportul pe care acestea sunt stocate și/sau transmise, precum și asupra documentelor de care au luat cunoștință, ca urmare a executării prezentului contract, atât pe perioada derulării prezentului contract, cât și ulterior, respectând reglementările legale in vigoare.

**ART.24** (1) O parte contractantă nu are dreptul fără acordul scris al celeilalte Părţi:

- de a face cunoscut contractul sau orice prevedere a acestuia unei terțe părți, în afara acelor persoane implicate în îndeplinirea contractului;
- de a utiliza informațiile și documentele obținute sau la care are acces în perioada de derulare a contractului, în alt scop decât acela de a-și îndeplini obligațiile contractuale.

(2)Dezvăluirea oricăror informaţii faţă de persoanele implicate în îndeplinirea contractului se va face confidenţial şi se va extinde numai asupra acelor informaţii necesare în vederea îndeplinirii contractului. Reprezentanții, angajații, resursele, colaboratorii, care au acces si trebuie să cunoască astfel de date și informații în vederea îndeplinirii obligațiilor asumate prin prezentul contract, vor fi instruiți asupra naturii confidențiale a termenilor și condițiilor prezentului contract precum și a datelor și informațiilor transmise în temeiul său.

**ART.25** O parte contractantă va fi exonerată de răspunderea pentru dezvăluirea de informaţii referitoare la contract dacă:

a) informaţia era cunoscută părţii contractante înainte ca ea să fi fost primită de la cealaltă parte contractantă, sau

b) informaţia a fost dezvăluită după ce a fost obţinut acordul scris al celeilalte părţi contractante pentru asemenea dezvăluire, sau

partea contractantă a fost obligată în mod legal să dezvăluie informaţia.

c) informaţia primită de la o parte a devenit publică între timp, fapt care poate fi probat;

d) informaţia primită de la una din Părţi a fost obţinută ulterior dintr-o altă sursă, în mod legal şi fără a încălca prezentul contract sau un altul similar cu acesta încheiat cu sursa în cauză; sau

e) astfel de informaţii au fost dezvoltate independent de cealaltă parte.

## X. DREPTURI DE PROPRIETATE INTELECTUALĂ

**ART.26** Prestatorul are obligaţia de a despăgubi Achizitorul împotriva oricăror:

a) reclamaţii şi acţiuni în justiţie ce rezultă din încălcarea unor drepturi de proprietate intelectuală (brevete, nume, mărci înregistrate etc.), legate de echipamentele, materialele, instalaţiile, utilajele sau programele folosite pentru sau în legatura cu prestarea serviciilor şi

b) daune - interese, costuri, taxe şi cheltuieli de orice natură, aferente, cu excepţia situaţiei în care astfel de încălcare rezultă din solicitarea scrisă explicită a Achizitorului.

## XI. CLAUZE DE FORŢĂ MAJORĂ

**ART.27** Forta Majoră exonerează de răspundere partea care o invocă, dar numai în măsura si pentru perioada în care partea este împiedicată sau întârziată să-şi execute obligaţiile din pricina situaţiei de Forţă Majoră.

**ART.28** Partea care invocă Forţa Majoră va notifica cealaltă Parte în scris în termen de cinci (5) zile de la apariţia situaţiei de Forţă Majoră prin oricare din modalităţile prevăzute în contract şi va dovedi cazul de Forţă Majoră în termen de zece (10) zile, pe bază de documente justificative emise de Camera de Comerţ şi Industrie a României. Încetarea situaţiei de Forţă Majoră va fi notificată în scris celeilalte Părţi într-un termen de maximum 10 zile de la data încetării.

**ART.29** (1) La primirea notificării mentionate mai sus, Părţile se vor consulta deîndată şi vor hotărî în termen de 48 ore asupra acţiunilor şi măsurilor ce trebuie întreprinse în scopul limitării sau depăşirii situaţiei de Forţă Majoră.

(2) Pentru nerespectarea obligaţiei de notificare a apariţiei cazului de Forţă Majoră, partea căreia îi revenea această obligaţie va răspunde pentru prejudiciile pe care cealaltă parte le-ar fi putut evita dacă ar fi fost anunţată în termen.

**ART.30** Dacă în termen de 10 zile de la producere, evenimentul de Forţă Majoră nu încetează, Părţile au dreptul să-şi notifice încetarea de plin drept a prezentului contract, fără ca vreuna dintre ele să pretinda daune-interese.

**ART.31** Părţile nu pot invoca Forţa Majoră atunci când se aflau în întârziere cu privire la îndeplinirea obligaţiei(iilor) înainte de producerea evenimentului de Forţă Majoră.

**ART.32** Părţile agreează ca apariţia unui caz fortuit, astfel cum este definit de lege, nu înlătură răspunderea Părţilor.

## XII. MODIFICAREA ŞI ÎNCETAREA CONTRACTULUI.

**ART.33** (1) De comun acord, părţile pot modifica prezentul contract printr-un înscris semnat de ambele părţi sub forma unui act adiţional.

**ART.34** (1) Prezentul contract încetează de plin drept fără intervenţia unei autorităţi şi instanţe de judecată, în următoarele situaţii:

a) pe baza acordului de voinţă a părţilor consemnat, in scris;

b) la expirarea perioadei de valabilitate pentru care s-a încheiat;

c) când în derularea contractului intervine o cauză de forță majoră constatată și invocată în condițiile legii.

d) prin denunțare unilaterală de către Achizitor, printr-o notificare prealabilă transmisă cu 15 zile înainte de data la care aceasta urmează să-și producă efectele.

(2) Contractul se reziliază fără intervenția instanței de judecată, în următoarele situații:

a) neîndeplinirea obligațiilor contractuale, situație care trebuie notificată părții care nu își îndeplinește obligațiile stabilite prin contract; rezilierea își va producele efectele în termen de 15 zile de la notificare daca pe durata acestui preaviz partea in culpa nu a remediat incalcarea respectiva;

b) una din părți a intrat în procedură de faliment, reorganizare sau lichidare.

(3) Rezilierea își produce efecte pentru viitor. Partea care în mod culpabil a dispus rezilierea contractului va suporta consecințele acestui fapt. În cazul angajării răspunderii contractuale, potrivit prevederilor prezentului articol, partea aflată în culpă este obligată la acoperirea integrală a prejudiciului.

(4) Rezilierea contractului nu va avea niciun efect asupra obligațiilor deja scadente între părți la data rezilierii.

(5) În cazul în care prezentul contract încetează înainte de expirarea perioadei contractuale din culpa Prestatorului, acesta va restitui Achizitorului valoarea rămasă pentru prestația neefectuată și achitată de către acesta.

(5) Prevederile cap. VII, VIII, IX, X, XIII, XIV din prezentul contract vor supraviețui încetării, pentru orice motive, a prezentului contract și vor produce efectele juridice care decurg din aplicarea lor.

## XIII. CLAUZA ANTICORUPȚIE ȘI DE EVITARE A CONFLICTULUI DE INTERESE

**ART.35** Prestatorul se obligă să ia toate măsurile necesare și rezonabile pentru a evita corupția și mita. În consecință, acesta nu va oferi, promite sau acorda și nu va determina un terț să ofere, să promită sau să acorde, prin intermediu angajaților, membrilor din conducerea acestora sau terților, beneficii sau alte avantaje (respectiv numerar, cadouri de valoare sau invitatii care nu au în principal scopuri profesionale, cum ar fi: evenimente sportive, concerte, evenimente culturale, vacante și alte asemenea) angajaților sau membrilor din conducerea Achizitorului, inclusiv rudelor acestora și altor persoane aflate in relatii stranse similar acestora.

**ART.36** În cazul unei încălcări grave a prezentei clauze, Achizitorul are dreptul să rezilieze unilateral, instantaneu, contractul existent fără preaviz și fără intervenția instanțelor judecătorești, respectiv are dreptul de a sesiza organele competente potrivit legii.

**ART.37** Prestatorul nu are dreptul de a angaja sau încheia orice alte înțelegeri privind prestarea de servicii, direct ori indirect, în scopul îndeplinirii contractului cu persoane fizice sau juridice care au fost implicate în procesul de verificare/evaluare a ofertelor depuse în cadrul procedurii de atribuire ori angajați ai Achizitorului sau implicați în procedura de

atribuire cu care Achizitorul a încetat relaţiile contractuale ulterior atribuirii contractului, pe parcursul unei perioade de cel puţin 12 luni de la încheierea contractului, sub sancţiunea rezoluţiunii ori rezilierii de drept a contractului.

## XIV. OBLIGAŢIILE PĂRŢILOR PRIVIND PROCESAREA DATELOR CU CARACTER PERSONAL

**ART.38** Părțile au luat la cunoștință de prevederile Regulamentului UE nr. 679/2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date - GDPR și se obligă să le respecte întocmai.

**ART.39** Părțile sunt de acord ca orice prelucrare a datelor cu caracter personal furnizate și utilizate pentru executarea contractului se va face doar în condițiile stipulate în GDPR, dreptul Uniunii Europene, precum și în conformitate cu legislația română în domeniul prelucrărilor de date cu caracter personal.

**ART.40** Părțile convin să prelucreze datele cu caracter personal asigurând măsuri tehnico-organizatorice adecvate de securitate conform GDPR.

**ART.41** Părțile sunt de acord să coopereze pe deplin în tratarea oricăror incidente care necesită notificarea autorității de supraveghere si/sau informarea persoanelor vizate afectate și să-și îndeplinească toate obligațiile legale în legătură cu această situație

**ART.42** Părțile au obligația de a respecta drepturile garantate ale persoanelor vizate.

## XV. DISPOZIŢII FINALE

**ART.43** (1) Anexa 1, Anexa 2 - Caietul de sarcini nr. 1958/08.05.2024 Revizia I și Anexa 3- Oferta prestatorului nr....., fac parte integrantă din prezentul contract.

(2) În cazul în care, pe parcursul executării contractului se constată că anumite elemente ale ofertei tehnice a prestatorului sunt inferioare sau nu corespund cerințelor prevăzute în caietul de sarcini prevalează prevederile Caietului de sarcini nr. 1958/08.05.2024 Revizia I.

**ART.44** Prestatorul are obligaţia de a nu transfera total sau parţial obligaţiile asumate prin contract fără acordul scris al celeilalte părţi.

**ART.45** Acest contract se supune legilor în vigoare în România.

**ART.46** Reprezentantul Prestatorului în acest contract declară că are toate împuternicirile necesare în conformitate cu legea română şi cu actele constitutive pentru semnarea, reprezentarea şi angajarea răspunderii Prestatorului.

**ART.47** Orice litigiu cu privire la executarea necorespunzătoare sau neexecutarea unei clauze contractuale intervenit în derularea prezentului contract va fi rezolvat pe cale amiabilă, iar în lipsa unui acord amiabil, litigiul va fi înaintat instanţelor judecătoreşti competente.

**ART.48** Părtile declară că au înțeles și acceptă în mod expres conținutul prezentului contract, inclusiv dar fără a se limita la următoarele clauze cap. III, IV, VII, XII, XIII, XIV.

**ART.49** Prezentul contract reprezintă voința liberă și neviciată a părților.

Contractul a fost semnat în 2 exemplare, ambele cu valoare de original, câte unul pentru fiecare parte, la București, la data de .....

**Prestator**

.....

**Administrator**

.....

**Achizitor**
**Societatea "INFORMATICĂ FEROVIARĂ" -SA**

**Director General**

.....

**Director Economic**

.....

**Director Departament Informatica**

.....

**Consilier Juridic**

.....

**Responsabil contract**

.....

Anexa 1

La contractul de prestări servicii nr .....

| Denumire serviciu | | | Cant. | Preţ unitar (lei fără TVA) | Valoare An 1 (lei fără TVA) | Valoare An 2 (lei fără TVA) | Valoare An 3 (lei fără TVA) | Valoare totalaă contract (lei fără TVA) |
|---|---|---|---|---|---|---|---|---|
| 1. Servicii de subscripţie antivirus + EDR | | | 1 | | | | | |
| 1.1 | 1.1.a Terminale din care | | 7.900 | | | | | |
| | 1.1.a1 | - Servere | 500 | | | | | |
| | 1.1.a2 | - Staţii de lucru | 7.400 | | | | | |
| | 1.1.b Cutii poştale | | 9.000 | | | | | |
| | Total valoare pct 1.1 (lei fără TVA) | | | | | | | |
| 1.2 | Servicii auxiliare de asistenţă configurare şi instruire | | 1 | | | | | |
| Valoare totală (lei fără TVA) | | | | | | | | |

Prestator

.....

Administrator

.....

Achizitor

Societatea "INFORMATICĂ FEROVIARĂ" -SA

Director General

.....

Director Economic

.....

Director Departament Informatica

.....

Responsabil contract

.....

F-10-029-12

# ÎMPUTERNICIRE*

Subscrisa ....., cu sediul în ....., înmatriculată la Registrul Comerţului sub nr. ....., CUI ....., atribut fiscal ....., reprezentată legal de ....., în calitate de ....., împuternicim prin prezenta pe ....., domiciliat în ....., identificat cu B.I./C.I. seria ....., nr. ....., CNP ....., eliberat de ....., la data de ....., având funcţia de ....., să ne reprezinte la procedura nr. ....., organizată de INFORMATICĂ FEROVIARĂ S.A. în scopul atribuirii contractului de .....

În îndeplinirea mandatului său, împuternicitul va avea următoarele drepturi şi obligaţii:

1. Să semneze toate actele şi documentele care emană de la subscrisa în legătură cu participarea la prezenta procedură;
2. Să participe în numele subscrisei la procedură şi să semneze toate documentele rezultate pe parcursul şi/sau în urma desfăşurării procedurii.
3. Să răspundă solicitărilor de clarificare formulate de către comisia de analiză în timpul desfăşurării procedurii.
4. Să depună în numele subscrisei contestaţiile cu privire la procedură.

Prin prezenta, împuternicitul nostru este pe deplin autorizat să angajeze răspunderea subscrisei cu privire la toate actele şi faptele ce decurg din participarea la procedură.

Notă: Împuternicirea va fi însoţită de o copie după actul de identitate al persoanei împuternicite (buletin de identitate, carte de identitate, paşaport).

Data .....

reprezentată legal prin

_____

**(Nume, prenume)**

_____

**(Funcţie)**

_____

**(Semnătura autorizată şi ştampila)**

*** Formularul se completează doar dacă documentele sunt semnate de o alta persoană desemnată de către administratorul societăţii.**

F-10-029-13

**OFERTANT**

.....

**(denumire)**

**DECLARAŢIE PRIVIND:**
**SITUAŢIA PERSONALĂ A OFERTANTULUI,**
**ÎNDEPLINIREA OBLIGAŢIILOR EXIGIBILE DE PLATĂ CĂTRE BUGETUL DE STAT ŞI BUGETUL LOCAL,**
**ÎNDEPLINIREA CRITERIILOR DE SELECŢIE**

1. Subsemnatul ....., reprezentant împuternicit al *(denumirea şi sediul ofertantului)*..... declar pe propria răspundere, sub sancţiunile aplicate faptei de fals în acte publice, că:

(I) Nu sunt în situaţia de a fi fost condamnat în ultimii 5 ani printr-o hotarâre judecătorească definitivă pentru următoarele infracţiuni:

a) constituirea unui grup infracţional organizat, prevăzută de art. 367 din Legea nr. 286/2009 privind Codul penal, cu modificările şi completările ulterioare

b) infracţiuni de corupţie, prevăzute de art. 289 - 294 din Legea nr. 286/2009, cu modificările şi completările ulterioare, şi infracţiuni asimilate infracţiunilor de corupţie prevăzute de art. 10 - 13 din Legea nr. 78/2000 pentru prevenirea, descoperirea şi sancţionarea faptelor de corupţie, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul ofertant a fost condamnat;

c) infracţiuni împotriva intereselor financiare ale Uniunii Europene, prevăzute de art. 18^1 - 18^5 din Legea nr. 78/2000, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul ofertant a fost condamnat;

d) acte de terorism, prevăzute de art. 32 - 35 şi art. 37 - 38 din Legea nr. 535/2004 privind prevenirea şi combaterea terorismului, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul ofertant a fost condamnat;

e) spălarea banilor, prevăzută de art. 29 din Legea nr. 656/2002 pentru prevenirea şi sancţionarea spălării banilor, precum şi pentru instituirea unor măsuri de prevenire şi combatere a finanţării terorismului, republicată, cu modificările ulterioare, sau finanţarea terorismului, prevăzută de art. 36 din Legea nr. 535/2004, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul ofertant a fost condamnat;

f) traficul şi exploatarea persoanelor vulnerabile, prevăzute de art. 209 - 217 din Legea nr. 286/2009, cu modificările şi completările ulterioare, sau de dispoziţiile corespunzătoare ale legislaţiei penale a statului în care respectivul ofertant a fost condamnat;

g) fraudă, în sensul articolului 1 din Convenţia privind protejarea intereselor financiare ale Comunităţilor Europene din 27 noiembrie 1995.

(2) Obligaţia de a exclude din procedura de atribuire un operator economic, în conformitate cu dispoziţiile alin. (1), se aplică şi în cazul în care persoana condamnată printr-o hotărâre definitivă este membru al organului de administrare, de conducere sau de supraveghere al respectivului operator economic sau are putere de reprezentare, de decizie sau de control în cadrul acestuia

**(II) Societatea nu se află** în nici una dintre situaţiile:

a) nu a încălcat reglementarile obligatorii în domeniul mediului, social şi al relaţiilor de muncă, stabilite prin legislaţia adoptată la nivelul Uniunii Eropene, legislaţia naţională, prin acorduri colective sau prin tratatele, convenţiile şi acordurile internaţionale în aceste domenii şi voi respecta aceste reglementări pe parcursul derulării contractului de achiziţie.

b) nu este în stare de faliment ori lichidare, afacerile nu îi sunt administrate de un administrator judiciar

c) activitaţile sale comerciale nu sunt suspendate sau în încetarea activităţii;

d) nu a comis o abatere profesională gravă care pune în discuţie integritatea (prin abatere profesională gravă se înţelege orice abatere comisă de ofertant care afectează reputaţia profesională a acestuia, cum ar fi încălcări ale regulilor de concurenţă de tip cartel care vizează trucarea licitaţiilor sau încălcări ale drepturilor de proprietate intelectuală, săvârşită cu intenţie sau din culpă gravă.)

e) nu am încheiat cu alţi operatori economici acorduri care vizează denaturarea concurenţei în cadrul sau în legătură cu procedura în cauză;

f) nu am participat la pregătirea procedurii de atribuire/participarea la pregătirea procedurii de atribuire nu a condus la o distorsionare a concurenţei.

g) nu a încălcat în mod grav sau repetat obligaţiile principale ce-i reveneau în cadrul unui contract de achiziţie cu Informatică Feroviară S.A., iar aceste încălcări au dus la încetarea anticipată a respectivului contract, plata de daune-interese sau alte sancţiuni comparabile;

h) nu a încercat să influenţeze în mod nelegal procesul decizional al Achizitorului, să obţină informaţii confidenţiale care i-ar putea conferi avantaje nejustificate în cadrul procedurii de atribuire.

i) nu se află într-o situație de conflict de interese în cadrul sau în legatura cu procedura în cauză.

j) nu prezintă informații false, nu a ascuns informații necesare pentru verificarea îndeplinirii criteriilor de selecție, nu va furniza cu întarziere documente justificative solicitate de Achizitor, nu a încercat să influențeze în mod nepermis procesul decizional al Achizitorului să obțină informații confidentiale care i-ar putea conferi avantaje necuvenite în cadrul procedurii, nu a furnizat din neglijență informații false care pot avea o influență semnificativă asupra deciziilor privind selecția și atribuirea sau nu prezintă informațiile solicitate de către achizitor.

III. Societatea a respectat obligațiile privind plata impozitelor, taxelor sau a contribuțiilor la bugetul general consolidat și nu înregistrează în acest moment, obligații de plată restante a impozitelor, taxelor și contribuțiilor de asigurări sociale la bugetul de stat și bugetul local;

De asemenea, mă oblig ca, în cazul în care sunt declarat câștigător, la solicitarea Achizitorului, să prezint în original sau conform cu originalul toate documentele solicitate în cererea de ofertă (certificat constatator ONRC, cazier judiciar și/sau certificatele de atestare fiscală privind achitarea obligațiilor exigibile, sau daca e cazul, să prezint documente privind eșalonarea acestora ori de alte facilități în vederea plății acestora, inclusiv, după caz, a eventualelor dobânzi ori penalități de întârziere acumulate sau a amenzilor).

IV. Îndeplinesc toate criteriile de selecție cu privire la capacitatea de a corespunde cerințelor, capacitatatea economică și financiară, capacitatea tehnică sau profesională solicitate de Achizitor la punctul. ..... din cererea de ofertă.

2. Subsemnatul declar că informațiile furnizate mai sus sunt complete și corecte în fiecare detaliu și mă oblig să furnizez la cerere și fără întârziere Achizitorului și/sau organizatorului procedurii, în scopul verificării și confirmării declarațiilor, orice forme de documente justificative, certificate privind situația personală a noastră precum și experiența, competența și resursele de care dispunem.

3. Subsemnatul autorizez, prin prezenta, orice instituție, societate comercială, bancă, alte persoane juridice, să furnizeze informații reprezentanților autorizați ai INFORMATICĂ FEROVIARĂ S.A., cu sediul în București, Str. Garii de Nord, nr. 1, sect.1, cu privire la orice aspect tehnic și financiar în legătură cu activitatea noastră.

Înțeleg că în cazul în care această declarație nu este conformă cu realitatea sunt pasibil de încălcarea prevederilor legislației penale privind falsul în declarații.

4. Prezenta declarație este valabilă până la data de *(se precizează data expirării perioadei de valabilitate a ofertei)*.....

**Data completării:** .....

_____

***(Nume, prenume)***

_____

**(Funcție)**

_____

**(Semnătura autorizată și ștampila)**

OFERTANT

.....

**(denumire)**

## INFORMAŢII GENERALE

1. Denumire: .....

2. Cod fiscal: .....

3. Adresa sediului central:

4. Telefon: .....
Fax: .....
E-mail: .....

5. Certificat de înmatriculare/înregistrare: .....
(număr, dată, loc de înmatriculare/înregistrare)

6. Obiect de activitate, pe domenii: .....
(în conformitate cu prevederile din statutul propriu)
7. Birourile filialelor/sucursalelor locale, dacă este cazul: .....
(adrese complete, telefon/fax, certificate de înmatriculare/înregistrare)

8. Principala piaţă a afacerilor: .....

9. Cifra de afaceri pe ultimii trei ani:

| Anul | Cifra de afaceri anuală (la 31.12) - lei - | Cifra de afaceri anuală (la 31.12) - echivalent euro - |
|---|---|---|
| 1. Anul 201.. | | |
| 2. Anul 201.. | | |
| 3. Anul 201.. | | |
| **Medie anuală:** | | |

**Data completării:** .....

_____
**(Nume, prenume)**

_____
**(Funcţie)**

_____
**(Semnătura autorizată şi ştampila)**

**OFERTANT**

.....

**(denumire)**

## EXPERIENŢA SIMILARĂ(*)

| | | |
|---|---|---|
| 1. Denumirea şi obiectul contractului:<br>Numărul şi data contractului: | | |
| 2. Denumirea beneficiarului/clientului:<br>Adresa beneficiarului/clientului:<br>Ţara: | | |
| 3. Calitatea în care a participat la îndeplinirea contractului:<br>*(se bifează opţiunea corespunzătoare)*<br>☐ contractant unic sau contractant conducător (lider de asociaţie)<br>☐ contractant asociat<br>☐ subcontractant | | |
| 4. Valoarea contractului<br><br>a) iniţială (la data semnării contractului):<br>b) finală (la data finalizării contractului): | Exprimată în moneda în care s-a încheiat contractul<br><br>.....<br><br>..... | Exprimată în echivalent euro<br><br>.....<br><br>..... |
| 5. Dacă au fost litigii privind îndeplinirea contractului, natura acestora şi modul lor de soluţionare: | | |
| 6. Cantitatea de produse care a fost furnizată în baza contractului: | | |
| 7. Natura produselor care au fost furnizată în baza contractului precum şi alte aspecte relevante prin care ofertantul îşi susţine experienţa similară: | | |

_____
*(Nume, prenume)*

_____
*(Funcţie)*

_____
*(Semnătura autorizată şi ştampila)*

(*) ***Se completează fişe distincte pentru fiecare contract în parte, care vor fi confirmate, la cererea comisiei de analiză, prin prezentarea contractului respectiv.***

**OFERTANT**

_____

**(denumirea)**

## DECLARAŢIE CONFLICT DE INTERESE

Subsemnatul(a) (denumirea, numele) ....., în calitate de ofertant / ofertant asociat / subcontractant propus / la procedura de (se menţionează procedura) ..... atribuirea contractului de achiziţie având ca obiect (denumirea seviciului şi codul CPV) ....., la data de (zi/lună/an)....., organizată de INFORMATICĂ FEROVIARĂ S.A., declar pe proprie răspundere, sub sancţiunea falsului în declaraţii, următoarele:

Nu ma aflu în situatii care să determine aparitia unui conflict de interese cu INFORMATICĂ FEROVIARA S.A., respectiv: orice situaţie în care membri personalului achizitorului, care sunt implicaţi în desfăşurarea procedurii de atribuire sau care pot influenţa rezultatul acesteia au, în mod direct sau indirect, un interes financiar, economic sau un alt interes personal, care ar putea fi perceput ca element care compromite imparţialitatea ori independenţa lor în contextul procedurii de atribuire.

Nu am drept membri în cadrul consiliului de administratie/organ de conducere sau de supervizare si/sau nu am actionari ori asociati persoane care sunt sot/sotie, ruda sau afin pana la gradul al doilea inclusiv sau nu ma aflu în relatii comerciale, cu persoanele ce detin functii de decizie în cadrul INFORMATICĂ FEROVIARĂ S.A. ;

Nu ma aflu în niciuna dintre situatiile precizate la lit. a)-e) de mai jos.

a) participarea în procesul de verificare/evaluare a ofertelor a persoanelor care deţin părţi sociale, părţi de interes, acţiuni din capitalul subscris al unuia dintre ofertanţi/subcontractanţi propuşi ori a persoanelor care fac parte din consiliul de administraţie/organul de conducere sau de supervizare al unuia dintre ofertanţi/ subcontractanţi propuşi;

b) participarea în procesul de verificare/evaluare a ofertelor a unei persoane care este soţ/soţie, rudă sau afin, până la gradul al doilea inclusiv, cu persoane care fac parte din consiliul de administraţie/organul de conducere sau de supervizare al unuia dintre ofertanţi/ ori subcontractanţi propuşi;

c) participarea în procesul de verificare/evaluare a ofertelor a unei persoane despre care se constată sau cu privire la care există indicii rezonabile/informaţii concrete că poate avea, direct sau indirect, un interes personal, financiar, economic ori de altă natură, sau se află

într-o altă situaţie de natură să îi afecteze independenţa şi imparţialitatea pe parcursul procesului de evaluare;

d) situaţia în care ofertantul /subcontractantul propus are drept membri în cadrul consiliului de administraţie/organului de conducere sau de supervizare şi/sau are acţionari ori asociaţi semnificativi persoane care sunt soţ/soţie, rudă sau afin până la gradul al doilea inclusiv ori care se află în relaţii comerciale cu persoane cu funcţii de decizie în cadrul INFORMATICĂ FEROVIARĂ S.A.; Prin acţionar sau asociat semnificativ se înţelege persoana care exercită drepturi aferente unor acţiuni care, cumulate, reprezintă cel puţin 10% din capitalul social sau îi conferă deţinătorului cel puţin 10% din totalul drepturilor de vot în adunarea generală.

e) situaţia în care ofertantul a nominalizat printre principalele persoane desemnate pentru executarea contractului persoane care sunt soţ/soţie, rudă sau afin până la gradul al doilea inclusiv ori care se află în relaţii comerciale cu persoane cu funcţii de decizie în cadrul INFORMATICĂ FEROVIARĂ S.A..

Subsemnatul declar că informaţiile furnizate sunt complete şi corecte în fiecare detaliu şi înţeleg că INFORMATICĂ FEROVIARĂ S.A. are dreptul de a solicita, în scopul verificării şi confirmării declaraţiilor, orice documente doveditoare de care dispun.

Înţeleg că în cazul în care această declaraţie nu este conformă cu realitatea sunt pasibil de încălcarea prevederilor legislaţiei penale privind falsul în declaraţii.

Persoanele cu funcție de decizie din cadrul INFORMATICĂ FEROVIARĂ S.A. sunt:

Numele și prenumele persoanelor din conducerea societății Radu Alexandru, Adrian Ambrosă, Viorel Daniel Purică, Cepleu Liliana, Ilie Mirabela Paulina.

Numele și prenumele membrilor comisiei de evaluare și a membrilor supleanți Cezar Cobianu, Mircea Galbenu,Florina Iftode, Tudor Florin, Mirela Natalia Dediu, Cezar Drob, Daniela Camelia Ungureanu.

Subsemnatul mă oblig să iau toate masurile necesare și rezonabile pentru a evita corupția ți mita. În consecință, nu voi oferi, promite sau acorda și nu voi determina un terț să ofere, să promita sau să acorde, prin intermediu angajatilor, membrilor din conducerea acestora sau terților, beneficii sau alte avantaje (respectiv numerar, cadouri de valoare sau invitații care nu au în principal scopuri profesionale, cum ar fi: evenimente sportive, concerte, evenimente culturale, vacanțe și alte asemenea) angajaților sau membrilor din conducerea INFORMATICĂ FEROVIARĂ S.A., inclusiv rudelor acestora și altor persoane aflate în relați strânse similar acestora.

În cazul în care voi fi declarat câștigător, și voi semna contractul de achiziție, nu voi angaja sau încheia orice alte înţelegeri privind prestarea de servicii, direct ori indirect, în scopul

F-10-029-18

**OFERTANT**

.....

**(denumire)**

## FORMULAR DE OFERTĂ FINANCIARĂ

Către: **Societatea "Informatică Feroviară" - S.A.**
**Str. Gării de Nord, Nr. 1, sector 1, Bucureşti**

1. Examinând Documentaţia procedurii, subscrisa (denumirea ofertantului) ..... ne oferim ca, în conformitate cu prevederile şi cerinţele cuprinse în documentaţie, să furnizăm :

| Denumire serviciu | | | Cant. | Preţ unitar (lei fără TVA) | Valoare An 1 (lei fără TVA) | Valoare An 2 (lei fără TVA) | Valoare An 3 (lei fără TVA) | Valoare totalaă contract (lei fără TVA) |
|---|---|---|---|---|---|---|---|---|
| 1. Servicii de subscripţie antivirus + EDR | | | 1 | | | | | |
| 1.1 | 1.1.a Terminale din care | | 7.900 | | | | | |
| | 1.1.a1 | - Servere | 500 | | | | | |
| | 1.1.a2 | - Staţii de lucru | 7.400 | | | | | |
| | 1.1.b Cutii poştale | | 9.000 | | | | | |
| | Total valoare pct 1.1 (lei fără TVA) | | | | | | | |
| 1.2 | Servicii auxiliare de asistenţă configurare şi instruire | | 1 | | | | | |
| Valoare totală (lei fără TVA) | | | | | | | | |

***La sumele respective se adaugă taxa pe valoare adăugată.***

2. Ne angajăm ca, în cazul în care oferta noastră este stabilită câştigătoare, să furnizăm produsele în conformitate cu prevederile contractuale.

3. Ne angajăm să menţinem această ofertă valabilă pentru o durată de (durata în litere şi cifre) ..... zile, respectiv până la data de

....., şi ea va rămâne obligatorie pentru noi şi poate fi acceptată oricând înainte de expirarea perioadei de valabilitate.

4. Până la încheierea şi semnarea contractului de achiziţie, această ofertă, împreună cu comunicarea transmisă de dumneavoastră, prin care oferta noastră este stabilită câştigătoare, vor constitui un contract angajant între noi.

5. Am înţeles şi consimţim ca, în cazul în care oferta noastră este stabilită ca fiind câştigătoare, să constituim garanţia de bună execuţie în conformitate cu prevederile din Invitaţia de participare la procedura Licitaţie nr. 2483/12.06.2024 şi „Caietul de sarcini" nr.1958/08.05.2024 (Revizia I).

6. Înţelegem că nu sunteţi obligaţi să acceptaţi oferta cu cel mai scăzut preţ sau orice altă ofertă pe care o puteţi primi.

**Data completării:** .....

Semnătura ..... în calitate de ....., autorizat să semnez oferta pentru şi în numele (denumire ofertant).....

F-10-029-19

**OFERTANT**

.....

*(denumire)*

**CERERE**

**de restituire a garanției de bună execuție**

***Către*: Informatică Feroviara S.A.**

Subscrisa ....., cu sediul în .....și CIF....., solicităm prin prezenta restituirea garanției de bună execuție, în valoare de ....., constituită în vederea executării contractului nr. .....prin:

☐ Scrisoare de garanție bancară nr. ..... emisă de .....

☐ Ordin de plată nr. .....

☐ Chitanța nr.....

☐ Alte forme de constituire, respectiv .....

.....

Restituirea garanției de bună execuție se va face .....

Vă mulțumim,

**Data completării:** .....

*(Nume, prenume)*

*(Funcție)*

*(Semnătura autorizată și ștampila)*

**Notă:** Cererea de restituire a garanției se va transmite în original la sediul Informatică Feroviară

# DECLARAȚIE DE ACCEPTARE A CONDIȚIILOR CONTRACTUALE

Subsemnatul.....(nume și prenume în clar a persoanei autorizate), reprezentant împuternicit al ..... (denumirea/numele și sediul/adresa candidatului/ofertantului), în nume propriu declar că sunt de acord cu toate prevederile modelului de contract prezentat în cadrul prezentei proceduri de atribuire și ne obligăm să respectăm toate obligațiile menționate în conținutul acestuia.

Data:

(numele si prenumele)_____,*(semnătura și stampilă)*,
în calitate de_____, legal autorizat să semnez
oferta pentru și în numele_____.

*(denumire/nume operator economic)*