

**APROBAT,**  
**Manager Departament TDI**  
*(semneaza pentru)*

**Macra**  
**Andreea**  
**-Anda**

Signed  
by Macra  
Andreea-Anda  
Date: 2026.06.04  
14:46:02 +03'00'

## CAIET DE SARCINI

**Servicii transport voce/date prin fibră optică**



## 1. INTRODUCERE

Caietul de sarcini face parte integrantă din Documentația de atribuire a acordului-cadru de furnizare servicii de transport voce/date prin fibră optică și cuprinde ansamblul cerințelor minimale și obligatoriu de îndeplinit, pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică, în condițiile în care criteriul de atribuire este "cel mai bun raport calitate-preț".

Cerințele impuse vor fi considerate ca fiind minime și obligatorii. În acest sens, orice ofertă prezentată, care se abate de la prevederile Caietului de sarcini, va fi luată în considerare, dar numai în măsura în care Propunerea tehnică presupune asigurarea unui nivel calitativ superior cerințelor minime din Caietul de sarcini. Ofertele care nu îndeplinesc toate cerințele minimale, specificate ca atare în caietul de sarcini, vor fi declarate neconforme. Nu se acceptă depunerea de oferte alternative. Nu se admit ofertele parțiale din punct de vedere cantitativ și calitativ, ci numai ofertele integrale, care corespund tuturor cerințelor stabilite prin prezentul caiet de sarcini.

Specificațiile tehnice care indică un anumit producător, o anumită origine sau un anumit procedeu ori care se referă la mărci, brevete, tipuri, la o origine sau la o producție specifică sunt menționate doar pentru identificarea cu ușurință a caracteristicilor serviciilor/produselor ce urmează a fi prestate/livrate și nu au ca efect favorizarea sau eliminarea anumitor operatori economici. Aceste specificații vor fi întotdeauna considerate ca având mențiunea «sau echivalent».

Pentru scopul prezentei secțiuni a Documentației de Atribuire, orice activitate descrisă într-un anumit capitol din Caietul de Sarcini și nespecificată explicit în alt capitol, trebuie interpretată ca fiind menționată în toate capitolele unde se consideră de către Ofertant că aceasta trebuia menționată pentru asigurarea îndeplinirii obiectului Contractului.

### 1.1. SITUAȚIA ACTUALĂ

Rețeaua de comunicații a HIDROELECTRICA constituie o infrastructură avansată, structurată dintr-o multitudine de segmente de rețea locală (LAN), interconectate prin canale specializate de comunicație, ceea ce conduce la formarea unei rețele extinse (WAN) de înaltă performanță. Acest ansamblu tehnologic permite o distribuție sigură și eficientă a resurselor informatice la nivelul întregii organizații.

Interconectarea segmentelor locale se realizează cu ajutorul echipamentelor de rețea esențiale (routere) care facilitează comutarea între diversele segmente și gestionează traficul de date în mod optim, asigurând un nivel ridicat de securitate, disponibilitate și redundanță a serviciilor de comunicații.

Prin intermediul acestei rețele extinse se derulează transmisii multiple, incluzând date operative, fluxuri video, servicii de voce și date pentru sistemele SCADA, esențiale pentru monitorizarea și automatizarea proceselor industriale.

Dintre aplicațiile critice care operează pe această infrastructură se remarcă:

- Serviciile de telefonie operativă – asigură comunicarea directă și rapidă între echipele operative din diferite locații, fiind vitală pentru coordonarea activităților de producție.
- HPMS/SCADA – suite de sisteme dedicate monitorizării, supravegherii și controlului automatizat al proceselor industriale, având un rol primordial în creșterea siguranței și eficienței operaționale.
- ERP/SAP – soluție integrată pentru managementul resurselor organizației, care optimizează procesele financiare, logistice, de resurse umane și administrative.
- Sistemul de videoconferință – facilitează colaborarea la distanță, luarea deciziilor în timp real și eficientizează procesele de management.

Prin această arhitectură solidă și modernă, SPEEH HIDROELECTRICA își consolidează capacitatea de a asigura comunicații eficiente, sigure și scalabile, susținând atât buna desfășurare a activităților interne, cât și relația cu partenerii și clienții săi.

## 2. OBIECTUL DOCUMENTAȚIEI

2.1. Se dorește achiziționarea de servicii de comunicații electronice prin atribuirea unui acord-cadru încheiat pe o perioadă de 4 ani, pe durata caruia se va perfecta un număr estimat de 4 (patru) contracte subsecvente, având ca obiect furnizarea: servicii de transport date/voce pe fibră optică.

## 2.2. DEFINIȚII

Definițiile de mai jos au ca scop determinarea încadrării juste a problemelor raportate de către SPEEH HIDROELECTRICA

În text, prescurtările următoare au semnificația:

NR. CRT.	ABREVIERE	DESCRIERE
1	DRP	Disaster Recovery Plan
2	BCP	Business Continuity Planning
3	SLA	Nivelul de Serviciu Agreat ( Service Level Agreement )
4	MPLS	Multiprotocol Label Switching
5	IP	Protocol Internet ( Internet Protocol )
6	VPN	Rețea virtuală privată ( Virtual private network )
7	ANCOM	Autoritatea Națională pentru Administrare și Reglementare în Comunicații
8	CCNA	Cisco Certified Network Associate
9	CCNP	Cisco Certified Network Professional
10	CCIE	Cisco Certified Internetwork Expert
11	CPE	Customer premises equipment
12	SIP	Session Initiation Protocol

## 3. CONDIȚII TEHNICE GENERALE PENTRU SERVICIILE FURNIZATE

### 3.1. SERVICII TRANSPORT VOCE/DATE

#### 3.1.1. CARACTERISTICI TEHNICE DE BAZA ALE SERVICIULUI IP VPN MPLS.

Soluția trebuie să dețină următoarele caracteristici (se aplică fiecărei locații):

- Soluția de transmisii de date trebuie să fie de tip VPN MPLS și să asigure comunicații de date de tip IP între sediul central al beneficiarului și locațiile acestuia din teritoriu.
- Se vor asigura conexiuni de nivel OSI 2 sau 3, interfața de conectare va respecta standardul 802.3 (Fast Ethernet și Gigabit Ethernet).

Comunicațiile de date proprii, interne, de tip IP nu vor fi furnizate prin intermediul rețelei Internet. Soluția va asigura doar planuri de adresare private fără a folosi translatarea de adrese/porturi, ofertantul urmând să folosească doar propria infrastructură IP MPLS. Ofertantul va furniza serviciul prin interfețe Ethernet (RJ-45) compatibile cu echipamentele din locațiile beneficiarului.

- Serviciile vor fi furnizate utilizând integral infrastructura proprie a ofertantului.
- Arhitectura rețelei VPN este de tip Any-to-Any.
- Se va asigura protocol dinamic de rutare pentru comutarea automată în cazul defectelor.
- Serviciul de transmisii de date de tip VPN MPLS oferit va include trafic nelimitat pe toată durata contractului.
- Soluția trebuie să fie scalabilă, în sensul adăugării de locații noi și up-grade bandă, la cererea Entității contractante, la aceleași tarife unitare oferite, urmând ca Entitatea contractantă să suporte și plata abonamentului lunar suplimentar corespunzător, conform ofertei financiare, începând cu data recepției serviciilor pentru locația respectivă/data de la care upgrade-ul de bandă devine disponibil.

- Dat fiind caracterul continuu al activității beneficiarului, care nu permite întreruperi în furnizarea serviciilor (24/24, 7/7, 365/365) iar furnizorul trebuie să asigure funcționarea echipamentelor de comunicație pe o perioadă de minim 3 ore în cazul lipsei tensiunii de alimentare.
- Ofertantul va asigura managementul centralizat al soluției 24/7/365 și monitorizarea proactivă a conexiunilor de date.
- Soluția de comunicații de tip VPN va respecta parametrii minimali pentru serviciile oferite, după cum urmează:
  - Întârzierea medie de transfer a pachetelor dus-întors: max. 100 ms (Delay);
  - Rata de pierdere a pachetelor: max. 1%(loss);
  - Variația întârzierii de transfer a pachetelor: max. 30ms (jitter)

Legătura va fi monitorizată non-stop de către personalul tehnic al prestatorului. Se va alerta personalul specializat al beneficiarului în cazul întreruperilor în furnizarea serviciului și se va deschide tichet de incident.

Furnizorul va asigura redundanța sistemului la nivel național cu descrierea modului în care se face aceasta.

### **3.1.2. CARACTERISTICI TEHNICE PRIVIND CANALELE DE COMUNICAȚIE**

Ofertantul va asigura canale de comunicație de tip punct la multi punct cu banda de transfer garantată. Nu se admit legături sau segmente de legături asigurate prin metode, tehnologii sau echipamente ce nu pot asigura un serviciu garantat.

Tipurile de servicii oferite de furnizori trebuie să nu fie în fază de teste. Se acceptă doar produse mature care să facă parte din oferta lor publică. Pentru aceasta Furnizorul va face dovada existenței serviciului "Circuite Virtuale Private" (sau echivalent).

Legătura între rețeaua Furnizorului și punctele de acces este realizată de furnizor cu echipamente și pe infrastructura proprie.

### **3.1.3. CERINȚE SUPORT TEHNIC ȘI DE MENTENANȚĂ.**

Specialiștii de suport ai furnizorului vor asigura asistența tehnică și mentenanța pentru echipamentele proprii prin intermediul cărora furnizează Entității contractante serviciile atât de la distanță cât și local, în funcție de necesități.

La solicitarea Entității contractante furnizorul va efectua, modificările în configurațiile echipamentelor prin intermediul cărora furnizează Entității contractante serviciile, ca urmare a schimbărilor în topologia rețelelor.

## **3.2. SERVICII TELEFONIE FIXĂ -SPECIFICATII TEHNICE MINIME OBLIGATORII**

**Pentru abonamentul linie telefonica principala – linie individuala:**

1. Serviciile de telefonie fixă vor fi prestate pentru numerele de apel actuale aparținând HIDROELECTRICA. Locațiile posturilor telefonice existente se regăsesc în Anexa 1 Tabel B.
2. Se vor preciza tarifele aferente acestui tip de abonament, detaliate, după cum urmează:
  - a) tarif abonament;
  - b) tarife pentru apelurile naționale în rețea proprie și în alte rețele de telefonie fixă și mobile;
  - c) tarife pentru convorbiri Internaționale;
  - d) alte tarife aplicabile pentru acest tip de abonament.
3. Alte precizări:

Se vor asigura următoarele servicii:

- numere de telefonie fixă din planul național de numerotație;
- acces la cerere pentru apeluri internaționale;

- posibilitatea limitării si/sau parolării de către autoritatea contractanta a apelurilor de ieșire pentru fiecare linie;
- număr de telefon neinformabil;
- apel in așteptare;
- apel programat;
- restricționarea identității liniei chemătoare;
- prezentarea identității liniei chemătoare;
- furnizarea serviciului 24h/24h, 7 zile pe săptămâna, 365 zile pe an;
- posibilitatea de a utiliza aparate pentru legături fax pe fiecare linie individuala, transmisiile fax având viteza de transmisie a datelor de la 9,6kbit/s pana la 33,6 kbps ;
- punerea la dispoziția autorității contractante a desfășurătorului convorbirilor telefonice o data cu transmiterea facturii;
- rezolvarea deranjamentelor in termen de 1 zi lucrătoare (24h) din momentul reclamării deranjamentului;
- trecerea la noul prestator de servicii se va face in aceeași zi pentru toate posturile de telefon si toate locațiile.
- autonomie de funcționare – minim 24h de la întreruperea tensiunii de rețea (220 VCA) in sediile Achizitorului, care intra in sarcina Prestatorului si nu implica resurse din partea Achizitorului.
- Se admit și legături de telefonie fixă peste rețeaua de telefonie mobilă cu acordul beneficiarului și cu asigurarea de terminale telefonice.
- Disponibilitatea serviciului minim 99,5%

#### **Alte precizări referitoare la serviciile de telefonie fixă:**

- Serviciile de telefonie fixă vor fi prestate pentru numerele de apel actuale. În cazul în care numerotația furnizorului de servicii nu corespunde cu numerotația actuală se va asigura portarea numerotației existente în rețeaua furnizorului.
- Serviciile vor fi furnizate utilizând integral infrastructura proprie a ofertantului, nu se accepta realizarea conexiunilor prin infrastructura subînchiriată de la alți operatori.
- Posturilor telefonice actuale sunt instalate in locațiile prezentate in Anexa 1 Tabel B la prezentul Caiet de sarcini;
- acces permanent la apeluri naționale, mobile;
- numere de telefonie fixă din planul național de numerotație pentru abonamentele noi,
- prestarea serviciului 24h/24h, 7 zile pe săptămână, 365 zile pe an;
- posibilitatea integrării serviciului oferit cu terminalele de fax existente în cadrul autorității contractante;
- posibilitatea conectării aparatelor fax (cu interfață RJ11) direct la linia telefonica (fără a fi necesare echipamente/adaptări si/sau aplicații software adiționale);
- PRESTATORUL de servicii integrate de telecomunicații va asigura autonomia si funcționarea liniei telefonice timp de 24 ore, in cazul unei pene de curent la locația AUTORITĂȚII CONTRACTANTE, indiferent de gradul de utilizare a acesteia – nefuncționalitățile datorate PRESTATORUL de servicii integrate de telecomunicații vor fi penalizate conform contractului. PRESTATORUL de servicii integrate de telecomunicații va prezenta soluția prin care va asigura autonomia liniei telefonice in condițiile menționate anterior
- punerea la dispoziția autorității contractante a desfășurătorului convorbirilor telefonice odată cu transmiterea facturii;
- Preluarea deranjamentului se va face prin apelarea gratuita din rețeaua Prestatorului a cel puțin unui număr de telefon si o adresa de email dedicata pentru suport tehnic. In oferta va fi descris

sistemul de asigurare a asistentei tehnice si de remediere a defecțiunilor. Se vor respecta următoarele valori:

- Timp de răspuns (max. 10 minut)
- Timp de notificare (max. 2 ore)
- Serviciile oferite vor avea disponibilitate de minim 99.5%. Nerespectarea acesteia va atrage penalizări conform contractului.
- Ofertantul va furniza serviciul de telefonie prin echipamentele aflate deja în dotarea autorității contractante (centrale telefonice si aparate telefonice/fax).
- Ofertantul va asigura continuitatea serviciului de telefonie fixa existent fără taxe de instalare si cheltuieli materiale si de manopera suplimentare, în situația câștigării ofertei.
- Entitatea contractantă poate solicita ulterior modificarea locațiilor sau a soluțiilor.

### 3.3. Cerințe privind Securitatea Informațiilor si măsuri tehnice și organizatorice pentru Protecția Datelor

Ofertantul se obliga sa respecte integral toate cerintele specificate în Anexa nr.3 privind securitatea informatiilor.

### 3.4. NIVELE ALE SLA-ULUI PENTRU TOATE SERVICIILE

Disponibilitatea garantată a serviciului este de minimum 99,5% lunar la fiecare din sediile Entitatii contractante; în cazul în care nu se respectă aceasta valoare, contractantul se obligă să acorde deduceri în factura lunii următoare conform tabelului de mai jos:

Tabel de compensații		
Disponibilitate Lunară*		Reducere din tariful de abonament lunar al Serviciului
Mai mare sau egal	Mai mic decât	%
95.00%	99.50%	15%
90.00	95.00%	30%
0.00%	90.00%	100%

Disponibilitatea serviciului se calculează lunar (în intervalul de livrare serviciu), pentru fiecare sediu în parte. Disponibilitatea Lunară\* se calculează după formula:

$$Disponibilitate\ lunară = \frac{Interval\_Livrare\_Serviciu - \sum Perioda\_Indisponibilitate}{Interval\_Livrare\_Serviciu}$$

Nu vor fi considerate perioade de indisponibilitate întreruperile planificate ale serviciului, anunțate de contractant cu minim 48 de ore înainte.

Nu vor fi considerate perioade de indisponibilitate întreruperile planificate ale serviciului, anunțate de contractant cu minim 48 de ore înainte.

Contractantul garantează o Disponibilitate minima a Serviciului pentru fiecare locație de 99,50%, ceea ce reprezintă o perioadă de întrerupere a serviciului de 3,6 ore în decursul a 30 zile (30 zile x 24ore = 720 ore x 0,5% = 3,6 ore).

Serviciul se va considera indisponibil pentru orice întrerupere totală și continuă de cel puțin 5 minute pentru un port sau o succesiune de minim 10 întreruperi într-o perioada de 30 minute.

Contractantul va livra periodic (lunar) către Beneficiar rapoarte scrise privind disponibilitatea serviciilor livrate. Rapoartele vor evidenția detalii privind incidentele – numărul bonurilor deschise la

Contractant de către Beneficiar, incluzând data și orele de deschidere și închidere ale acestor intervenții, detalii despre rezoluția intervenției.

### 3.5. Timpi de remediere

Entitatea contractantă a definit trei nivele de clasificare ale incidentelor în funcție de gradul de severitate și numărul de locații unde se produce deranjamentul. La fiecare semnalare a unui Incident/ Deranjament, acesta este repartizat într-una dintre aceste categorii. În aceste situații se aplică următoarele definiții:

PRIORITATE	DESCRIERE
<b>CRITIC</b> Pierdere de serviciu	Probleme care afectează grav serviciul, capacitatea traficului și necesită acțiuni corective imediate.
<b>MAJOR</b> Afectează calitatea serviciul furnizat și funcționarea rețelei	Degradarea parțială a serviciului. Degradarea funcționării sistemului sau a serviciului, care are un impact semnificativ asupra calității serviciilor.
<b>MINOR</b> Nu afectează serviciul furnizat sau funcționarea	Probleme minore care nu reduc funcționarea sistemului sau serviciului. Problema este tolerabilă în timpul utilizării sistemului.

Timpii maximali de remediere/restabilire a serviciului sunt:

CRITIC: 4 h

MAJOR: 24 h

MINOR: 72 h

Timp de răspuns pentru înregistrarea unei reclamații privind indisponibilitatea serviciului calculat de la momentul primirii emailului/telefonului de la beneficiar până la înregistrarea acesteia: maxim 10 de minute.

Depășirea timpilor maximali ofertati de remediere/restabilire a serviciului duce la penalități după cum urmează:

Tabel de compensații nerespectare timpi de remediere		
Timp de remediere mai mare decât cel maxim oferat		Reducere din tariful de abonament lunar al Serviciului pt locațiile afectate
Mai mare sau egal	Mai mic decât	%
0 ore	3 ore	15%
3 ore	6 ore	30%
6 ore	12 ore	100%

„Suport tehnic de urgenta”, pentru rezolvarea indisponibilităților sistemului clasificate ca evenimente **Critice**.

„Suport tehnic în timpul programului normal de lucru”, pentru asistenta la izolarea sau rezolvarea problemelor cu un grad de impact redus; investigarea și rezolvarea problemelor ne-legate de Produs; consultanta privind funcționarea sistemului și configurarea acestuia, precum și întrebări tehnice.

„Asistenta tehnica on-site”, este asigurată prin deplasarea specialiștilor furnizorului în obiectivele S.C. Hidroelectrică S.A. atunci când se consideră necesar pentru rezolvarea unei probleme raportate.

“Suport tehnic de urgenta” - Furnizorul va asigura suport tehnic de urgenta 24 de ore pe zi, 7 zile pe săptămâna, inclusiv zilele libere oficial recunoscute pentru rezolvarea indisponibilităților de sistem clasificate ca evenimente **Critice**.

„Suport tehnic în timpul programului normal de lucru” – Furnizorul va asigura suport tehnic în timpul programului normal de lucru de luni pana vineri între orele 08:00 și 18:00, în vederea rezolvării oricărui tip de evenimente.

#### 4. ALTE CERINȚE MINIME

4.1. Furnizorul va asigura menținerea în funcțiune a rețelei montând echipamentele proprii astfel încât să îndeplinească condițiile de disponibilitate a serviciilor solicitate de Entitatea contractantă.

Furnizorul asigură funcționarea echipamentelor de comunicație pe o perioadă de minim 3 ore în cazul lipsei tensiunii de alimentare, pe toată perioada de derulare a acordului cadru.

În timpul operațiilor de montaj și configurare, întreruperile anunțate în funcționarea rețelei nu trebuie să depășească 6 ore.

Întreruperile vor fi programate în perioada de sfârșit de săptămână pentru a nu perturba activitatea curentă a societății noastre.

4.2. Furnizorul declarat castigator va fi responsabil pentru migrarea serviciilor actuale in propria retea. Migrarea se va executa fara costuri suplimentare pentru Entitatea contractanta si intra in responsabilitatea furnizorului. Serviciile vor fi livrate catre Entitatea contractanta fara intreruperi si fara impactarea calitatii serviciilor si a parametrilor de functionare. Timpul de indisponibilitate la migrarea serviciilor, intre momentul intreruperii la furnizorul anterior si momentul inceperii functionarii serviciilor la nou, se va incadra in conditiile SLA.

Timpul de instalare a serviciului reprezinta intervalul de timp de la transmiterea cererii de activare/ instalare catre Furnizor, pana la confirmarea functionalitatii de catre Entitatea contractanta, prin acceptanta (excluzand intarzierile datorate Entitatii contractante). Instalarea tuturor serviciilor ce fac obiectul prezentului caiet de sarcini, se va realiza in termen de maximum 30 de zile de la semnarea primului contract subsecvent.

In cazul in care, pe perioada unui contract subsecvent Entitatea contractanta solicita activarea de servicii suplimentare/modificarea (diminuare/majorare/modificari de banda) celor deja contractante, instalarea acestora/modificarea se va realiza in termen de maximum 15 zile de la data primirii de catre furnizor a solicitarii emise de Entitatea contractanta in acest sens.

#### 5. IPOTEZE SI RISCURI

Riscuri identificate in procesul de elaborare a Caietului de sarcini.

Riscuri asociate furnizorului:

<b>Refuzul / Imposibilitatea de a semna contractul atribuit cu consecințe asupra finalizării procedurii prin încheierea contractului</b>	<ul style="list-style-type: none"><li>- Constituirea din etapa de planificare / pregătire a procesului de achiziție a unei Garanții de Participare in condițiile prevăzute de art. 41-42 din HG nr. 394/2016</li><li>- Aplicarea dispozițiilor art. 149, alin.(2) din HG nr. 394/2016</li></ul>
<b>Riscul de nerealizare parțială sau totală a recepției serviciilor prestate</b>	<ul style="list-style-type: none"><li>- Constituirea unei garanții de buna execuție a contractului, in condițiile art. 45, alin.(1), alin.(3) si alin.(4) din HG nr. 394/2016 (5 % din valoarea contractului)</li></ul>
<b>Riscul de îndeplinire defectuoasă a obligațiilor contractuale.</b>	<ul style="list-style-type: none"><li>- Atenționarea responsabilului de contract al furnizorului cu privire la îndeplinirea defectuoasă a obligațiilor contractuale.</li><li>Aplicarea de penalități in conformitate cu Caietul de sarcini si Contractul semnat.</li></ul>

## Riscuri asociate autorității contractante

### 1. Neefectuarea recepției serviciilor prestate în termenele asumate prin contract

- Comunicarea contractului perfectat tuturor părților interesate (responsabilii de contract nominalizați).

## 6. PROBE ȘI RECEPȚIE

Se vor efectua minim următoarele teste și probe funcționale, verificări și măsurători:

- Verificarea integrității canalelor de comunicație;
- Măsurarea parametrilor "pierderi de pachete date" și "întârziere pachete in rețea";
- Verificarea benzii minime garantate;
- Verificarea efectuării de convorbiri telefonice (dacă este cazul);
- Verificarea efectuării de videoconferința (dacă este cazul);
- Verificare funcționării echipamentelor de telecomunicații timp de 3 ore în lipsa alimentării

locale la rețeaua de energie electrică;

- Verificarea aplicațiilor de monitorizare (dacă este cazul);

Verificarea funcționării noilor servicii contractate se face pe o durată de maximum 5 zile lucratoare, stabilită de comun acord (fără costuri din partea Entității contractante – deplasare pe locație, costuri de verificare a serviciilor contractate etc.), în baza unui plan de verificare, elaborat de Furnizor și aprobat de reprezentanții locali desemnați ai Entității contractante. După verificare, predarea se va face în baza unui Proces verbal de punere în funcțiune, care va cuprinde, acolo unde este cazul, rezultatele testelor și probelor funcționale, semnat de ambele părți. Recepția serviciilor se va efectua numai cu condiția realizării parametrilor ceruți și numai după terminarea probelor de punere în funcțiune, acolo unde este cazul.

Furnizorul se obligă să întreprindă toate acțiunile ( proiectare, avize, lucrări, mutare, migrare, portare, livrare echipamente în custodie, instalare, configurare, etc.) necesare finalizării testelor de recepție a serviciilor instalate, corespunzătoare celor existente și funcționale la Entitatea contractantă la data contractării și care trebuie să fie finalizate cel mai târziu în termen de maximum 30 de zile de la data perfectării primului contract subsecvent. Furnizorul este responsabil pentru soluțiile tehnice aplicate, fiind sancționat pentru întreruperile de trafic sau degradarea serviciului. Furnizarea serviciului în condiții tehnice ce nu acoperă cerințele impuse prin prezentul caiet de sarcini, este considerată ca indisponibilitate sau întrerupere în furnizarea serviciului.

În cazul în care furnizorul, din vina sa, nu reușește să îndeplinească obligațiile asumate privind termenele de realizare a lucrărilor pentru furnizarea serviciilor, achizitorul are dreptul de a aplica oricare dintre sancțiunile contractuale, fără alte obligații.

Disponibilitatea și conformitatea serviciilor prestate lunar cu cerințele caietului de sarcini vor fi verificate și recepționate lunar de către Entitatea contractantă (prin reprezentanții locali ai acesteia).

În cazul instalării unor echipamente/servicii noi, punerea lor în funcțiune și recepția lor se va face în baza unui set de teste propus de Furnizor și aprobat de Entitatea contractantă până la data operaționalizării serviciilor noi contractate. Furnizorul este responsabil cu elaborarea unui plan de testare în vederea verificării conformității și recepționării noilor servicii contractate. Testele de recepție a serviciilor contractate vor fi făcute de Furnizor în prezența reprezentanților Entității contractante, cu echipamentele de măsură și control puse la dispoziție de Furnizor.

Recepția livrabilelor se va realiza pe întreaga durată de derulare a contractelor subsecvente conform calendarului de mai jos:

Etapa	Rezultat / Livrabil	Termen Recepție	Plată (% din val. servicii)
Mobilizare	Plan de implementare, și grafic portare (unde e cazul)	30 zile de la data perfectării contractului	Incluse in abonamentul lunar

<b>Echipamente</b>	Livrarea și recepția terminalelor (telefoane/tablete) și a SIM-urilor	30 de zile de la solicitarea Entității contractante	Inclusă în prețul abonamentelor
<b>Activare (pentru toate tipurile de servicii)</b>	Raport de activare/portare reușită pentru toate liniile de voce și date	30 de zile de la data perfectării contractului/ 15 zile de la solicitarea Entității contractante pentru servicii suplimentare/modificare de servicii	(începerea facturării lunare a abonamentelor)
<b>Testare (pentru toate tipurile de servicii)</b>	Raport de acceptanță tehnică (verificare acoperire, viteză date în locațiile solicitate)	30 zile + 5 zile de la data perfectării contractului	Incluse în abonamentul lunar
<b>Operare (pentru toate tipurile de servicii)</b>	Livrarea primului set de rapoarte de consum lunare	Lunar pe întreaga durată de derulare a contractului subsecvent	Plată lunară abonamente (recurent)

### 7. Cantități și cerințe pentru serviciile transport voce/date prin fibra optica

Sucursala Râmnicu Valcea are nevoie de un sistem suplimentar de linii de comunicații pentru a asigura redundanța comunicațiilor. La fel și UHE Caransebes, UHE Tg.Jiu, UHE Oradea, UHE Sibiu, există locații care se afla foarte aproape de magistrala de fibra optica la care pot fi conectate. De asemenea la Sucursala Curtea de Arges se dorește o soluție de telefonie terestra pe suport de fibra optica, acolo unde locațiile se afla foarte aproape de magistrale de fibra optica la care pot fi conectate.

Furnizorul va asigura legături de comunicație permanente între punctele prevăzute în Anexa 1 tabel A. Furnizorul va asigura servicii de telefonie fixa pe suport fibra optica în punctele prevăzute în Anexa 1 tabel B

Furnizorul va asigura o soluție de conectare securizată între nodurile rețelei care să asigure viteze de transport pe liniile de comunicație conform Anexa 1 cu posibilității de majorare.

Pe durata acordului-cadru se estimează cantitățile minime și maxime după cum urmează:

Nr. crt.	Tipul serviciului	Cantitate minima	Cantitate maxima
1	Transport voce date	20	45
2	Servicii de telefonie Fixa	1	2

Primul contract subsecvent al acordului cadru se va încheia pentru următoarele cantități

Nr. crt.	Tipul abonamentului	Cantitate	Detalii
1	Transport voce date	37	Anexa 1 tabel A
2	Servicii de telefonie fixa	2	Anexa 1 tabel B

### SPECIFICATII TEHNICE MINIME OBLIGATORII

Ofertantul va asigura furnizarea canalelor de comunicații VPN MPLS conform cerințelor minime specificate la cap. 3, utilizând ca suport fizic exclusiv rețele de fibră optică. Totodată, serviciile de telefonie fixă vor fi furnizate prin intermediul aceleiași infrastructuri de fibră optică.

### 8 OBLIGAȚIILE ȘI RESPONSABILITĂȚILE PĂRȚILOR

În raport cu produsele solicitate și cu cerințele stipulate în prezentul Caiet de Sarcini, obligațiile și responsabilitățile părților sunt:

#### 8.1. Ofertantul are următoarele obligații principale:

- de a garanta și livra serviciile și produsele în conformitate cu cerințele din caietul de sarcini și specificatiile tehnice;

- b. de a garanta ca echipamentele prin care se asigura serviciile furnizate prin contract respecta legislatia Romana si Europeana din punct de vedere tehnic, securitate, mediu;
- c. Prestatorul se obliga sa pastreze confidentialitatea asupra informatiilor de orice natura la care are acces prin desfasurarea activitatilor prevazute in acest contract, conform legislatiei in vigoare, inclusiv privind Protectia Datelor cu Caracter Personal;
- d. mobilizarea de resurse suficiente și cu expertiză adecvată pentru a asigura gestionarea contractului, astfel cum este solicitat la nivelul Caietului de Sarcini,
- e. îndeplinirea obligațiilor contractuale, cu respectarea bunelor practici din domeniu, a prevederilor legale și contractuale relevante, astfel încât să se asigure că obligațiile sunt îndeplinite la parametrii solicitați,
- f. asigurarea unui grad de flexibilitate în planificarea modalității de gestionare a contractului, pe toată durata de derulare a contractului,
- g. transmiterea datelor de identificare și de contact ale personalului alocat pentru executarea contractului
- h. colaborarea cu personalul entității contractante alocat pentru verificarea serviciilor furnizate si/sau a produselor livrate și realizarea recepțiilor,
- i. reducerea, în măsura posibilă, la minim, a situațiilor de întârzieri în efectuarea furnizării serviciilor, minimizând astfel impactul negativ asupra activității entității contractante,
- j. asigurarea că orice documente, documentații și/sau instrucțiuni furnizate către personalul entității contractante sunt exacte și elaborate în conformitate cu bunele practici specifice în domeniu,
- k. prezentarea rapoartelor solicitate de personalul entității contractante, potrivit cerințelor de raportare stabilite prin Contract,

Obligațiile principale ale Ofertantului devenit Contractant se completează cu obligațiile prevăzute în condițiile contractuale.

### **8.2. Entitatea contractantă are următoarele obligații principale:**

- a. desemnarea unei persoane sau a unei echipe pentru monitorizarea contractului,
- b. punerea la dispoziția Contractantului a tuturor informațiilor disponibile și necesare pentru derularea contractului în timpul stabilit și la nivelul de calitate și performanță prevăzut în Caietul de Sarcini,
- c. asigurarea accesului în spațiile în care urmează a se realiza, după caz instalarea produselor;
- d. mobilizarea tuturor resurselor care sunt în sarcina sa, pentru buna derulare a contractului,
- e. colaborarea cu Contractantul pentru a identifica în timp util orice eventuale probleme care ar putea apărea pe parcursul derulării contractului,
- f. asigurarea acurateței oricăror informații puse la dispoziția Contractantului pe durata derulării contractului,
- g. monitorizarea îndeplinirii tuturor cerințelor din Caietul de Sarcini și a oricăror elemente ale Propunerii Tehnice și Financiare pe durata derulării contractului, efectuarea și păstrarea unei arhive cu înregistrări pentru documentarea nivelului de performanță a Contractantului,
- h. notificarea Contractantului prin canalele de comunicație puse la dispoziție de acesta privind orice incidente sau disfuncționalități care intervin pe perioada de derulare a contractului,
- i. verificarea tuturor documentelor asociate recepției produselor și serviciilor suport care fac obiectul contractului, respectiv care confirmă furnizarea serviciilor de comunicatii si/sau a produselor potrivit condițiilor de calitate stabilite în Caietul de sarcini.

## 9 Cadrul legal care guvernează relația dintre entitatea contractantă și contractant (inclusiv în domeniile mediului, social și al relațiilor de muncă)

Ofertantul devenit contractant are obligația de a respecta obligațiile aplicabile în domeniul mediului, social și al muncii instituite prin dreptul Uniunii, prin dreptul național, prin acorduri colective sau prin dispozițiile internaționale de drept în domeniul mediului, social și al muncii enumerate în anexa X la Directiva 2014/24, respectiv:

- i. Convenția nr. 87 a OIM privind libertatea de asociere și protecția dreptului de organizare;
- ii. Convenția nr. 98 a OIM privind dreptul de organizare și negociere colectivă;
- iii. Convenția nr. 29 a OIM privind munca forțată;
- iv. Convenția nr. 105 a OIM privind abolirea muncii forțate;
- v. Convenția nr. 138 a OIM privind vârsta minimă de încadrare în muncă;
- vi. Convenția nr. 111 a OIM privind discriminarea (ocuparea forței de muncă și profesie);
- vii. Convenția nr. 100 a OIM privind egalitatea remunerației;
- viii. Convenția nr. 182 a OIM privind cele mai grave forme ale muncii copiilor;
- ix. Convenția de la Viena privind protecția stratului de ozon și Protocolul său de la Montreal privind substanțele care epuizează stratul de ozon;
- x. Convenția de la Basel privind controlul circulației transfrontaliere a deșeurilor periculoase și al eliminării acestora (Convenția de la Basel);

## 10 Managementul / Gestionarea Contractului și activități de raportare în cadrul Contractului

Prin responsabilul de contract, desemnat de Entitatea contractantă, respectiv prin account managerul desemnat de furnizorul de servicii se asigură managementul Contractului, ce include o componentă de management și o componentă administrativă – de administrare efectivă a Contractului – și presupune coordonarea continuă, monitorizarea și controlul tuturor activităților și rezultatelor realizate de Contractant.

Pe parcursul derulării Contractului, Entitatea contractantă verifică la intervale stabilite și comunicate prin Caietul de sarcini dacă toate activitățile planificate au fost realizate conform termenelor/cerințelor și că serviciile au fost furnizate la standardele solicitate și acceptate.

Monitorizarea activităților contractului se realizează prin:

- raportare periodică -furnizorul transmite lunar lunar un **Raport SLA (SLA Report)** care centralizează toți indicatorii (Uptime, latență, tichete de suport rezolvate),
- Entitatea contractantă poate efectua teste de viteză și disponibilitate pentru validarea datelor din Raportul SLA, plata serviciilor urmând a fi corelată cu datele din Raportul SLA.

Pentru fiecare tip de serviciu se vor urmări următoarele componente cheie de monitorizare a contractului.

### Servicii VPN

Managementul contractului	Activitati de raportare	Frecvență
Monitorizarea Disponibilității (Uptime): Verificarea automată a stării nodurilor de rețea și a legăturilor de date (24/7).	Raport SLA Procentul de uptime realizat vs. cel contractat; timpii medii de răspuns la incidente.	Lunar
Monitorizarea Consumului: Urmărirea cotelor de trafic (date mobile/fixe) pentru a evita depășirile de cost neprevăzute.	Raport de incidente - Lista tuturor deranjamentelor, cauza rădăcină (root cause) și timpul de remediere pentru fiecare	lunar

## Servicii voce fixă

Managementul contractului	Activitati de raportare	Frecvență raportare
Activarea/dezactivarea serviciilor, portarea numerelor (daca este cazul)	Rapoarte lunare de utilizare	lunar
Urmărirea nivelului de disponibilitate a serviciului conform cerințelor	Rapoarte de trafic (destinatii apelate/durata medie apeluri)	lunar
Timp de raspuns la SLA	Raport SLA	lunar

### 11 Modalități și condiții de plată

Entitatea contractantă se obligă față de Furnizor să plătească prețul convenit pentru furnizarea de către Furnizor a serviciilor recepționate, respectiv acceptate de Entitatea contractantă, în termenul convenit în contract, în baza documentelor ce atestă prestarea serviciilor și acceptarea acestora de către Entitatea contractantă.

Plățile în cadrul contractelor subsecvente vor fi recurente, corelate cu graficul de monitorizare și raportare precizat în tabelul de la cap. 10 din prezentul caiet de sarcini.

Factura va fi emisă în lei, cu TVA, pe baza prețurilor unitare specificate în contract.

Factura va avea menționat numărul și data contractului, datele de emisie și de scadență ale facturii. De asemenea, în facturile emise pentru operațiunile realizate în baza contractului, se vor înscrie, în mod obligatoriu, codurile CPV corespunzătoare prevăzute în nomenclatorul de referință în domeniul achizițiilor publice, adoptat prin Regulamentul (CE) nr. 2.195/2002 al Parlamentului European și al Consiliului din 5 noiembrie 2002 privind Vocabularul comun privind achizițiile publice (CPV).

Entitatea contractantă va efectua plata facturii prin virament în contul de trezorerie al Contractantului, în termen de maxim 30 de zile de la data primirii facturii sau, în cazul în care factura a fost primită anterior finalizării recepției cantitative și calitative, în termen de maxim 30 de zile de la data finalizării recepției cantitative și calitative.

### 12 Instrucțiuni privind elaborarea ofertei

Caietul de sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor minime pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică. Cerințele impuse vor fi considerate ca fiind minime. Oferta Tehnică va fi elaborată în limba română, într-o formă tabelară, cu răspuns punctual la fiecare cerință din Caietul de sarcini pentru componentele alese.

Furnizorul va elabora Oferta Financiară astfel încât aceasta să furnizeze toate informațiile cu privire la preț, completând Formularul- Centralizator de prețuri. Prețul va fi exprimat în lei (RON fără TVA) și va avea maximum 2 zecimale.

Propunerea financiară va fi elaborată sub formă tabelară, cu răspuns punctual și ferm la fiecare tip de serviciu solicitat.

Oferta financiară va conține tarifele pentru furnizarea fiecărui tip de serviciu cu includerea tuturor echipamentelor și accesoriilor necesare furnizării serviciului (inclusiv echipamentele terminale, antenele necesare, etc), în condițiile specificate în Caietul de Sarcini. Serviciile vor fi oferite astfel încât toate cheltuielile să fie acoperite.

### 13 ANEXELE denumite:

Anexa 1 - Servicii transport voce/date prin fibra optica

Anexa 2 - Factori și algoritmi de evaluare a ofertelor

Anexa 3 - Cerințe privind Securitatea Informațiilor și măsuri tehnice și organizatorice pentru Protecția Datelor, parte integrantă din prezentul Caiet de sarcini

Verificat,  
Șef Serv. TDI  
Bogdan Iosif ON



Întocmit,  
Analist programator Serv. Strategie Digitală  
Alice FLORESCU



Expert Serv. Cyber Security  
Gheorghe VLĂDOIU



## Anexa 1 Conexiuni Fibra Optica

Tabel A Transport voce / date :

Nr.crt.	Start	Destinatie	Latitudine	Longitudine	Lățime de banda minim garantata
1.	Sediul SH Rm. Vâlcea		45°07'16.99"N	24°22'07.63"E	100 Mbps
2.	Sediul SH Rm. Vâlcea	CHE Gura Lotrului	45°20'40.94"N	24°16'30.43"E	50 Mbps
3.	Sediul SH Rm. Vâlcea	CHE Turnu	45°16'36.92"N	24°18'34.12"E	50 Mbps
4.	Sediul SH Rm. Vâlcea	CHE Călimănești	45°14'25.00"N	24°20'49.11"E	50 Mbps
5.	Sediul SH Rm. Vâlcea	CHE Dăești	45°10'41.73"N	24°22'7.82"E	50 Mbps
6.	Sediul SH Rm. Vâlcea	CHE Răureni	45° 4'15.63"N	24°21'42.78"E	50 Mbps
7.	Sediul SH Rm. Vâlcea	CHE Govora	45° 0'34.13"N	24°17'48.29"E	50 Mbps
8.	Sediul SH Rm. Vâlcea	CHE Băbeni	44°54'59.88"N	24°14'44.29"E	50 Mbps
9.	Sediul SH Rm. Vâlcea	CHE Ionești	44°51'15.01"N	24°14'47.63"E	50 Mbps
10.	Sediul SH Rm. Vâlcea	CHE Zăvideni	44°46'22.16"N	24°16'20.86"E	50 Mbps
11.	Sediul SH Rm. Vâlcea	CHE Drăgășani	44°40'53.76"N	24°17'35.59"E	50 Mbps
12.	Sediul SH Rm. Vâlcea	Dep. Călimănești	45°14'9.10"N	24°21'12.60"E	50 Mbps
13.	Sediul SH Rm. Vâlcea	MHC Prislop	45°12'47.11"N	24° 1'44.46"E	50 Mbps
14.	Sediul SH Rm. Vâlcea	CHE CORNETU	45.392811	24.307124	50 Mbps
15.	Sediu UHE Dorin Pavel		45°23'14.27"N	23°56'49.62"E	100 Mbps
16.	Sediu UHE Dorin Pavel	CHE Malaia	45°21'13.00"N	24° 1'28.33"E	50 Mbps
17.	Sediu UHE Dorin Pavel	CHE Brădișor	45°21'9.27"N	24° 7'2.28"E	50 Mbps
18.	Sediu UHE SLATINA		Str. Tudor Vladimirescu, nr. 158, cod:230087, Slatina, Jud. Olt		100 Mbps
19.	Sediu UHE SLATINA	CHE Strejești	44.535715	24.322186	50 Mbps
20.	Sediu UHE SLATINA	CHE Arcești	44.447076	24.312990	50 Mbps
21.	Sediu SH Hateg		45.611746	22.956604	100 Mbp
22.	Sediu SH Hateg	Baraj Gura Apelor	45.338953	22.715954	50 Mbps
23.	Sediu UHE Caransebes		Str. Splai Sebeș, nr. 2A, cod:325400, Caransebeș, Jud. Caras Severin		100 Mbp
24.	Sediu UHE Caransebes	MHC MARGA	45,480465	22,540785	10 Mbps

25.	Sediu UHE Caransebes	CHE Raul Alb( nod presiune Raul Alb )	45.184196 (45.182175 )	22.366696 ( 22.369969 )	50 Mbps
26.	Sediu UHE Caransebes	CHE Ruieni (stația 110 KV. Turnu Ruieni )	45.40928769 ( 45.410147 )	22.34662886 ( 22.346983 )	50 Mbps
27.	Sediu UHE Caransebes	Baraj Măru si CHE Măru	45.427910 ( 45.427044 )	22.478087 ( 22.472174 )	50 Mbps
28.	Sediu UHE Caransebes	Transelectrica Iaz	45.502780	22.296223	50 Mbps
29.	Sediu UHE Tg.Jiu		45.051271	23.274731	100 Mbp
30.	Sediu UHE Tg.Jiu	CHE Tismana Aval	45.044382°	22.947579°	50 Mbps
31.	Sediu UHE Tg.Jiu	CHE Târgu Jiu	45.032562°	23.263486°	50 Mbps
32.	Sediu UHE Tg.Jiu	CHE Vădeni	45.057830°	23.268460°	50 Mbps
33.	Sediul UHE Oradea		Str. Ogorului, nr.34, Oradea, jud. Bihor		100 Mbps
34.	Sediul UHE Oradea	CHE Remeti	46.830532°	22.684460°	50 Mbps
35.	Sediul UHE Oradea	CHE Munteni	46.873838°	22.682934°	50 Mbps
36.	Sediu UHE Sibiu		45.777354	24.158176	100 Mbp
37.	Sediu UHE Sibiu	CHE Sadu 5	45,60151332738479	24,00153037058384	50 Mbps

**Tabel B Servicii telefonie Fixa.**

1.	CHE Clăbucet	45.489605	25.148777
2.	Baraj Satic	45.443313	25.170334

## Anexa 2 - Factori si algoritm de evaluare a ofertelor

Criteriul de atribuire selectat: Cel mai bun raport calitate - preț, în conformitate cu prevederile art. 209 alin. (3) lit. a) din Legea nr. 99/2016, cu modificările și completările ulterioare.

Factorii de evaluare a ofertelor și punctajele alocate

Nr. crt.	Factori de evaluare	Punctaj maxim alocat
1.	a.Componenta financiară: Prețul ofertei*	85 puncte
2.	b.Componenta tehnică: Timpul de remediere/restabilire a serviciului	10 puncte
3.	c. Componenta tehnică: Acces la sistemul de ticketing al furnizorului	5 puncte
Total		100 puncte

\*valoarea maximă ce ar putea fi atinsă pe durata Acordului-cadru

Punctajul pentru factorul de evaluare „Prețul ofertei” se acordă astfel:

- pentru cel mai mic preț ( $P_{\min}$ ) se acordă punctajul maxim alocat (85 de puncte);
- pentru prețurile oferite ( $P_{\text{oferta}}$ ) mai mari decât  $P_{\min}$  punctajul acordat se calculează astfel:

$$P(n) = (P_{\min} / P_{\text{oferta}}) \times 85$$

unde:

- $P(n)$  = punctajul acordat ofertei analizate;
- $P_{\min}$  = valoarea ofertei cu prețul cel mai scăzut;
- $P_{\text{oferta}}$  = valoarea ofertei analizate

Punctajul pentru factorul de evaluare „Timpul de remediere/restabilire a serviciului” –  $P_{Tr}$  – 10 puncte, se acordă astfel:

Descriere factor-Punctajul se acorda in functie de tipul de incident (conform clasificarii de la cap. 3.1.5. din caietul de sarcini) si timpul de remediere oferat.

Punctaj pentru incidentele critice maxim 4 puncte ( $P_{\text{Crit}}$ ):

Tip de incident	Timp de remediere oferat		Punctaj acordat
	Mai mare sau egal cu	Mai mic decât	
Critic	½ h	1h	4
Critic	1h	1,5 h	3
Critic	1,5 h	2,5 h	2
Critic	2,5	3,5 h	1
Critic	3,5 h	4	0,5

Pentru un timp de remediere oferat de 4h oferta este conformă dar va primi 0 puncte.

Punctaj pentru incidentele majore maxim 4 puncte ( $P_{\text{Maj}}$ ):

Tip de incident	Timp de remediere oferat		Punctaj acordat
	Mai mare sau egal cu	Mai mic decât	
Major	6 h	10 h	4
Major	10 h	15 h	3
Major	15 h	18 h	2
Major	18 h	20 h	1
Major	20h	24 h	0,5

Pentru un timp de remediere ofertat de 24 oferta este conformă dar va primi 0 puncte.

*Punctaj pentru incidentele minore maxim 2 puncte ( $P_{Min}$ ):*

Tip de incident	Timp de remediere ofertat		Punctaj acordat
	Mai mare sau egal cu	Mai mic decât	
Minor	26 h	30 h	2
Minor	30h	40h	1.5
Minor	40 h	50 h	1
Minor	50h	60 h	0.5
Minor	60	72h	0.25

Pentru un timp de remediere ofertat de 72 h oferta este conformă dar va primi 0 puncte.

Punctajul total al factorului de evaluare „Timpul de remediere/restabilire a serviciului” se face prin insumarea punctajelor de la fiecare tip de incident in parte:

$$P_{Tr} = P_{Crit} + P_{Maj} + P_{Min}$$

*Punctajul pentru factorul de evaluare „Acces la sistemul de ticketing al furnizorului” –  $P_{Ast}$  – 5 puncte, se acordă astfel:*

*Descriere factor - Deranjamentele vor fi anunțate pe email și/sau telefonic. In scopul îmbunătățiri managementului conexiunilor, furnizorul poate asigura, suplimentar, accesul personalului tehnic al Entității contractante la sistemul propriu de ticketing pentru vizualizare incidente tehnice, crearea de tickete și urmărirea rezolvării acestora.*

Pentru ofertarea unei solutii care asigură accesul personalului tehnic al Entității contractante la sistemul propriu de ticketing al furnizorului suplimentar fata de modalitățile de anuntare mail/telefonic punctajul acordat ( $P_{ast}$ ) este de 5 de puncte;

Pentru ofertarea unei solutii care asigură ca modalități de anuntare doar e-mail/ telefonic punctajul oferta este conformă dar nu se acordă punctaj.

#### DECLARAREA OFERTEI CÂȘTIGĂTOARE

În urma procesului de evaluare a ofertelor, se va întocmi un clasament, în ordinea descrescătoare a punctajului total, calculat conform algoritmului descris mai sus.

În cazul în care două sau mai multe oferte sunt clasate pe primul loc, cu punctaje egale, departajarea se va face având în vedere punctajul obținut la factorii de evaluare în ordinea descrescătoare a ponderilor acestora. În situația în care egalitatea se menține, autoritatea contractantă va solicita noi propuneri financiare și oferta câștigătoare va fi desemnată cea cu propunerea financiară cea mai mică.

## **Anexa 3 - Cerințe privind Securitatea Informațiilor și măsuri tehnice și organizatorice pentru Protecția Datelor**

### **1. Cerințe privind Securitatea informațiilor**

Cerințele globale sunt cerințe care se aplică, în general, furnizării tuturor serviciilor de către FURNIZOR.

#### **1.1. Surse recunoscute**

FURNIZORUL se asigură că echipamentele pe care le operează sunt obținute din surse cunoscute și renumite și că există un suport tehnic fiabil pentru acestea.

#### **1.2. Guvernanța în domeniul securității**

FURNIZORUL stabilește, menține și monitorizează un cadru de guvernanță în materie de securitate a informațiilor, care permite organului de conducere al FURNIZORULUI să stabilească o direcție clară și să demonstreze angajamentul său față de securitatea informațiilor și gestionarea riscurilor.

#### **1.3. Managementul Riscurilor Informaționale**

FURNIZORUL se asigură că (i) înainte de implementarea unor noi medii IT care găzduiesc informații ale Entității Contractante inclusiv date personale (numite în continuare „informațiile Entității Contractante”, (ii) înainte de implementarea unor modificări majore la cele existente, și (iii) introducerea unor tehnologii semnificativ noi, riscurile de securitatea informațiilor asociate sunt evaluate, tratate, monitorizate și păstrate în limite acceptabile. Informațiile referitoare la activitățile de gestionare a riscurilor sunt partajate fără întârziere cu Entitatea Contractantă, la cerere.

#### **1.4. Managementul Securității**

FURNIZORUL (i) a stabilit o funcție de specialist în securitatea informațiilor, condusă de un manager cu puteri decizionale suficiente, căruia îi sunt încredințate autoritatea și resursele adecvate pentru a asigura aplicarea eficientă și consecventă a bunelor practici privind securitatea informațiilor în întreaga companie și pentru a asigura respectarea cerințelor juridice, de reglementare și contractuale care afectează securitatea informațiilor. FURNIZORUL (ii) menține un program cuprinzător, actualizat, de conștientizare în domeniul securității, pentru a promova și a integra comportamentul așteptat privind securitatea în raport cu toate persoanele care au acces la informațiile Entității Contractante.

#### **1.5. Proceduri Operaționale Documentate**

FURNIZORUL a stabilit responsabilități și proceduri pentru administrarea și operarea serviciilor sale pentru a se asigura că o astfel de documentare este (i) conformă cu standardele din industrie și bunele practici recunoscute, (ii) documentată în mod adecvat în scris și (iii) actualizată în orice moment în cursul aplicării prezentului Acord.

#### **1.6. Managementul activelor**

FURNIZORUL se asigură că (i) activele (hardware și software) pe care le operează, numite în continuare active, care sunt folosite pentru a crea, procesa, stoca sau transmite informații ale Entității Contractante sunt protejate împotriva coruperii, pierderilor, furtului și divulgării neautorizate pe tot parcursul ciclului lor de viață. FURNIZORUL se asigură că aceste active sunt înregistrate într-un registru care este (ii) protejat împotriva modificărilor neautorizate, (iii) actualizat, (iv) copiat periodic (backup) și (v) conține detaliile necesare privind activele și include - dacă este cazul - cerințele de conformitate

referitoare la active. FURNIZORUL se asigură că (vi) toate activele sunt alocate unui proprietar care este responsabil pentru operarea (exploatarea) activului.

#### 1.7. Accesul la sistem

FURNIZORUL restricționează accesul la activele în care informațiile Entității Contractante sunt create, procesate, stocate sau transmise persoanelor autorizate în scopuri de business specifice. Aceasta include cel puțin faptul că (i) doar utilizatorii autorizați pot avea acces la informații ale Entității Contractante; (ii) privilegiile de acces sunt limitate la funcționalitatea aprobată a sistemului; (iii) există o separare adecvată a sarcinilor; (iv) privilegiile de acces nu sunt atribuite colectiv (numele de utilizator și parolele să poată fi partajate). FURNIZORUL se asigură că accesul administrativ la sistemele care stochează sau procesează informațiile Entității Contractante este (v) limitat la un număr minim de administratori, (vi) protejat prin procedura de autentificare în doi pași sau în cazul în care autentificarea în doi pași nu este posibilă din punct de vedere tehnic, măsuri de securitate echivalente (de ex. parole generate temporar în sistemele de management). FURNIZORUL se asigură de asemenea că accesul administrativ este (vii) întotdeauna înregistrat pentru a permite detectarea și investigarea accesului neautorizat și a manipulării neautorizate a informațiilor Entității Contractante. (viii) Mai mult decât atât, FURNIZORUL se asigură că există o procedură oficială în vigoare, care descrie modul în care sunt create, revizuite în mod regulat, modificate, blocate și șterse rolurile, conturile, drepturile de acces și privilegiile privind accesul administrativ.

#### 1.8. Managementul Sistemului

FURNIZORUL administrează sisteme care creează, stochează, procesează sau transmit informații ale Entității Contractante pentru a (i) face față volumului de muncă curent și preconizat și (ii) le configurează într-o manieră consecventă și precisă pentru a le proteja pe ele și informațiile Entității Contractante pe care le procesează, stochează sau transmit împotriva funcționării defectuoase, atacului cibernetic, divulgării neautorizate, coruperii, furtului și pierderii. FURNIZORUL gestionează securitatea sistemelor prin (iii) efectuarea de copii de rezervă a informațiilor esențiale și a software-ului, (iv) aplicarea unui proces riguros de gestionare a modificărilor și (v) monitorizarea acordurilor la nivel de servicii convenite.

#### 1.9. Rețele și comunicații

FURNIZORUL asigură proiectarea rețelelor prin care oferă serviciile de comunicații, pentru ca acestea să fie (i) fiabile și rezistente, (ii) să împiedice accesul neautorizat, (iii) să utilizeze conexiuni criptate și (iv) să detecteze traficul suspect. (v) FURNIZORUL asigură configurarea dispozitivelor de rețea pe care le pune la dispoziția Entității Contractante în scopul furnizării serviciilor solicitate pentru a funcționa conform cerințelor și pentru a preveni actualizările neautorizate și incorecte. FURNIZORUL asigură protejarea sistemelor de comunicații electronice prin (vi) stabilirea politicii de utilizare a acestora, (vii) configurarea setărilor de securitate, (viii) securizarea infrastructurii tehnice de sprijin. (ix) FURNIZORUL asigură ascunderea rețelelor și a topologiilor față de terți. FURNIZORUL se asigură că restricționează accesul extern la sistemele și rețelele informatice ale Entității Contractante prin (x) rutarea traficului de rețea prin firewall-uri sau firewall-uri proxy, (xi) limitarea metodelor de conectare la minimul necesar, (xii) acordarea accesului doar la aplicațiile de business autorizate, la sistemele informatice sau la anumite părți ale rețelei.

#### 1.10. Separarea Sistemelor și Serviciilor de comunicații

FURNIZORUL se asigură că sistemele și serviciile de comunicații sunt cel puțin izolate logic, astfel încât să se reducă riscul accesului neautorizat sau al modificării neautorizate.

#### 1.11. Scanarea de Vulnerabilități

FURNIZORUL se asigură că (i) sistemele operate de acesta sunt testate în mod regulat împotriva vulnerabilităților și a defecțiunilor de configurare prin efectuarea de teste dinamice (teste de penetrare sau scanări de vulnerabilități). (ii) Toate rezultatele acestor teste relevante pentru Entitatea Contractantă sunt partajate cu Entitatea Contractantă fără întârziere; (iii) vulnerabilitățile critice vor fi raportate la Entitatea Contractantă imediat. (iv) FURNIZORUL oferă asistență și sprijin pentru auditul patch-urilor de securitate și a managementului vulnerabilităților realizat de Entitatea Contractantă. (v) Atenuarea vulnerabilităților de securitate va fi efectuată pe baza nivelului de risc și a intervalelor de timp convenite între părți.

#### 1.12. Nivele de patch-uri actualizate

FURNIZORUL asigură remedierea vulnerabilităților tehnice prin administrarea unui proces de gestionare a patch-urilor pentru echipamentele pe care acesta le operează și care asigură furnizarea serviciilor (i) identificarea și obținerea de patch-uri din surse autorizate, imediat ce acestea sunt disponibile, (ii) decizia când pot fi distribuite patch-urile, (iii) patch-uri de testare pe baza unor criterii cunoscute, (iv) distribuirea patch-urilor în timp util, (v) înregistrarea de patch-uri care au fost aplicate într-o baza de date de management al configurărilor (CMDB).

#### 1.13. Cerințe Minime de Autentificare

FURNIZORUL se asigură că cerințele minime ale Entității Contractante pentru autentificare (autentificarea în doi pași) sunt impuse prin intermediul soluției Entității Contractante pentru mediul IT utilizat pentru stocarea sau procesarea informațiilor Entității Contractante. Trebuie aplicat principiul celor mai puține privilegii și necesitatea de a cunoaște și separarea sarcinilor. Mai mult, trebuie aplicat un model de control al accesului bazat pe roluri.

#### 1.14. Cerințe de Proiectare a Rețelei

Trebuie să existe o arhitectură multi-nivel iar segmentele de rețea trebuie să fie separate de segmentele de nivel scăzut și mediu cu măsuri de securitate adecvate pentru a preveni traficul de date între segmente. Segmentul de rețea pentru nivelul foarte ridicat trebuie să fie, de asemenea, separat și securizat față de segmentele pentru nivelurile ridicate.

#### 1.15. Criptarea

Datele în repaus și datele în mișcare (în tranzit) vor fi stocate și transmise numai utilizând protocoale securizate și criptare de ultimă generație. Datele de autentificare (parole, PIN-uri) pot fi transmise doar criptate prin rețea. În plus, transporturile fizice ale suporturilor de stocare trebuie să fie securizate prin protecție fizică și criptare.

#### 1.16. Securizare (Hardening)

Toate echipamentele de rețea trebuie securizate. Aceasta include (i) dezactivarea serviciilor, instrumentelor, protocoalelor și interfețelor inutile, (ii) ștergerea sau cel puțin schimbarea numelor de utilizator și a parolelor implicite, (iii) activarea opțiunilor de sporire a securității și (iv) prevenirea transferului de informații tehnice către entități externe.

#### 1.17. Înregistrarea evenimentelor de securitate

Pentru a permite detectarea și investigarea accesului neautorizat și a manipulării neautorizate a informațiilor Entității Contractante, FURNIZORUL se asigură că (i) înregistrarea evenimentelor este activată permanent pentru toate sistemele operate de acesta pentru a crea, stoca, procesa sau transmite informații ale Entității Contractante, (ii) sistemele sunt configurate astfel încât să genereze evenimente legate de securitate și evenimente relevante pentru integritatea datelor (inclusiv tipuri de evenimente cum ar fi modificări la informațiile Entității Contractante, încercările de conectare

reușită și nereușită a utilizatorilor, crearea / modificarea / ștergerea serviciului, crearea / modificarea / ștergerea obiectelor, disfuncționalitatea sistemului, ștergerea conturilor de utilizator) precum și atributele asociate fiecărui eveniment (de exemplu data, ora, ID-ul utilizatorului, numele fișierului și adresa IP), (iii) sursele coerente de date și de timp fiabile asigură că jurnalele de evenimente utilizează mărci temporale precise (de exemplu: prin utilizarea serverelor NTP), (iv) jurnalele de evenimente de securitate și evenimente relevante pentru integritatea datelor sunt protejate împotriva accesului neautorizat și modificării/suprascrierii accidentale sau intenționate, (v) jurnalele de evenimente de securitate vor fi puse la dispoziția Entității Contractante, la cerere.

#### 1.18. Managementul Conformității

FURNIZORUL se asigură că toate sistemele pe care acesta le operează în scopul furnizării serviciilor sunt scanate periodic, pentru a respecta "Politicile/ Standardele de Securitate proprii ale FURNIZORULUI conform reglementarilor ANCOM.

#### 1.19. Eliminarea Securizată și Reutilizarea

FURNIZORUL se asigură că hardware-ul pe care acesta îl operează și care urmează a fi dezafectat este (i) fie complet șters înainte de a fi reutilizat, vândut sau returnat astfel încât toate informațiile Entității Contractante să fie șterse în întregime în condiții de siguranță (ii) sau este distrus în condiții de siguranță. (iii) Ștergerea completă sau distrugerea trebuie realizată într-un mod securizat, utilizând cele mai moderne tehnologii și practici, cum ar fi instrumentele și practicile definite în NIST 800-88 "Ghid pentru formatarea suporturilor media". (iv) Conceptele pentru eliminarea și ștergerea securizată, precum și dovezile privind eliminarea și ștergerea securizată a bunurilor informaționale ale Entității Contractante sunt partajate cu Entitatea Contractantă, la cerere.

#### 1.20. Securitatea Resurselor Umane

Pentru fiecare persoană care acționează în numele FURNIZORULUI și căreia i se acordă permisiuni de acces (la nivel local sau de la distanță), informațiile de identificare a persoanei trebuie puse la dispoziția Entității Contractante. FURNIZORUL asigură o verificare a identității persoanelor și că nimeni nu abuzează de accesul sau permisiunea acordată persoanelor respective de către FURNIZOR. FURNIZORUL se asigură că autorizațiile acordate sunt imediat retrase după încetarea sau schimbarea persoanelor și/ sau responsabilităților. În plus, FURNIZORUL își asumă responsabilitatea pentru orice daune produse datorită accesului neautorizat și / sau utilizării informațiilor Entității Contractante. FURNIZORUL delegă doar personalul care este calificat în mod demonstrabil pentru sarcinile necesare.

## 2. Cerințe referitoare la protecția datelor

### 2.1. Angajamentul față de confidențialitate

Furnizorul va instrui toți angajații proprii care prelucrează date cu caracter personal ale Entității Contractante sau au acces la aceste date în ceea ce privește securitatea datelor și protecția datelor. Dacă este legat de o cerință legală, FURNIZORUL obligă angajații în scris să păstreze secretul privind telecomunicațiile (în conformitate cu Directiva Europeană nr. 58/2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice – ePrivacy Directive - sau reglementări privind confidențialitatea electronică în versiunea lor validă, coroborat cu normele naționale privind secretul telecomunicațiilor, de exemplu Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice.

FURNIZORUL va instrui toți angajații care prelucrează date cu caracter personal ale Entității Contractante sau au acces la aceste date în ceea ce privește securitatea datelor și protecția datelor. Participarea va fi documentată pe bază de nume specific.

## 2.2. Protecția datelor prin design

FURNIZORUL va stabili reglementări privind „Protecția datelor prin design” pentru a lua în considerare dreptul la protecția datelor în dezvoltarea și proiectarea produselor, serviciilor și aplicațiilor (de exemplu, prin măsuri precum minimizarea datelor, pseudonimizarea, setările implicite pentru protecția datelor).

## 2.3. Responsabil pentru protecția datelor

În conformitate cu cerințele legale (articolele 37-39 GDPR și legislația națională), este desemnat un responsabil cu protecția datelor.

Responsabilii cu protecția datelor nu trebuie să aibă niciun conflict de interese.

Responsabilul cu protecția datelor deține calificările și experiența necesare pentru compania specifică.

Conducerea sprijină responsabilul cu protecția datelor.

Responsabilul cu protecția datelor este subordonat direct conducerii și raportează direct acesteia.

Responsabilul cu protecția datelor este informat și implicat în planificarea noilor procese sau modificarea proceselor existente în timp util.

Responsabilul cu protecția datelor participă activ la proiectarea proceselor.

## 2.4. Sistemul de management al protecției datelor

FURNIZORUL a stabilit un sistem de management al protecției datelor care respectă cerințele GDPR și este supus unui proces continuu de testare și îmbunătățire.

În ceea ce privește procesarea datelor cu caracter personal, analiza riscurilor este efectuată pe baza unor criterii definite și transparente, iar riscurile la adresa protecției datelor și securității informațiilor sunt identificate, evaluate și gestionate corespunzător în cadrul unui proces stabilit în mod obligatoriu și aplicat continuu pe baza acestor criterii. Managementul este complet informat și integrat într-o organizație de protecția datelor și securitatea informațiilor, precum și în procesele respective de comunicare, escaladare și decizie, și se asigură că sarcinile și responsabilitățile pot fi îndeplinite în măsura necesară și la un nivel de calitate satisfăcător.

Sunt puse la dispoziție resurse suficiente pentru stabilirea, implementarea, derularea, monitorizarea, analizarea, menținerea și îmbunătățirea sistemului de management al protecției datelor și există o dovadă a disponibilității acestora.

Este garantat faptul că doar personalul care are calificări concrete suficiente pentru a înțelege sarcinile alocate este implicat în operarea sistemului de management al protecției datelor. Acest lucru este asigurat prin instruirii și prin alte măsuri de pregătire.

## 3. Conformitate

FURNIZORUL se obligă ca toate facilitățile de găzduire a datelor și de suport în care informațiile Entității Contractante sunt stocate sau prelucrate să fie operate și să asigure cerințele de securitate în conformitate cu ISO/IEC 27001 “Tehnologia informației – Tehnici de securitate – Sisteme de Management a Securității Informațiilor - Cerințe”.

FURNIZORUL este de acord să partajeze "Declarația de aplicabilitate" cu Entitatea Contractantă înainte de data intrării în vigoare, la reînnoirea sa și în concordanță cu solicitările făcute de Entitatea Contractantă în orice moment pe parcursul derulării prezentului Acord.

FURNIZORUL este de acord să asigure că "Declarația de aplicabilitate" acoperă toate facilitățile de găzduire și operare, aplicațiile și procesele unde informațiile Entității Contractante sunt prelucrate sau stocate.

FURNIZORUL se angajează să respecte, cu strictețe, toate prevederile și cerințele stabilite de Directiva NIS 2, asigurându-se că atât termenii, cât și metodele de implementare sunt aplicate în mod corespunzător și conform normelor actuale. Această obligație presupune alinierea proceselor interne și a politicilor de securitate la standardele europene specifice, cu accent pe protecția rețelelor și a sistemelor informatice care sunt esențiale pentru furnizarea serviciilor sale.

În vederea respectării Directivei NIS 2, FURNIZORUL va adopta măsuri concrete pentru identificarea, evaluarea și gestionarea riscurilor legate de securitatea cibernetică, va documenta toate acțiunile întreprinse și va asigura monitorizarea continuă a conformității. De asemenea, va colabora strâns cu Entitatea Contractantă pentru raportarea promptă a incidentelor de securitate, comunicarea vulnerabilităților identificate și implementarea unor soluții eficiente pentru atenuarea acestora, garantând astfel o protecție sporită a datelor și a infrastructurii digitale pe întreaga durată a Acordului.

#### 4. Interfețele Procesului de Securitate IT

Ambele părți sunt de acord să comunice și să pună la dispoziție persoane de contact pentru următoarele procese de securitate IT:

- Managementul Conformității: Pentru a schimba informații cu privire la respectarea cerințelor, a furniza în mod constant certificate și rapoarte, astfel cum sunt definite în prezenta Anexă, și a discuta și a conveni asupra acțiunilor de gestionare a neconformităților existente și a riscurilor aferente. La cerere, Entitatea Contractantă poate solicita furnizarea de informații specifice privind respectarea cerințelor de către subcontractanții FURNIZORULUI, dacă este cazul.
- Managementul Incidentelor de Securitate IT și breșele privind datele personale: Pentru a schimba informații privind incidentele de securitate IT sau evenimentele de securitate IT care ar putea conduce la un incident de securitate IT care afectează sau ar putea afecta mediul IT utilizat pentru stocarea sau procesarea informațiilor Entității Contractante. "Managementul incidentelor de securitate IT" include, de asemenea, gestionarea solicitărilor de expertiză /emise de către Entitatea Contractantă. Breșele privind datele cu caracter personal și incidentele de securitate IT cu relevanță pentru protecția datelor trebuie raportate de FURNIZOR către Entitatea Contractantă imediat, dar cel puțin în termenul legal stabilit; în acest sens, se face trimitere la dispozițiile relevante ale acordului de protecție a datelor.
- Managementul Riscurilor: Pentru a schimba informații privind activitățile de gestionare a riscurilor efectuate de FURNIZOR pentru a asigura în mod corespunzător identificarea, evaluarea, gestionarea, monitorizarea și menținerea într-o limită acceptabilă, în mod permanent, a riscurilor legate de securitatea informațiilor.
- Managementul Vulnerabilităților: Pentru a schimba informații privind vulnerabilitățile care afectează sau ar putea afecta mediul IT utilizat pentru stocarea sau procesarea informațiilor Entității Contractante și pentru a discuta și a conveni asupra acțiunilor de atenuare a vulnerabilităților existente.
- Managementul Patch-urilor: Pentru a schimba informații privind ferestrele de mentenanță aprobate și distribuirea de patch-uri.
- Managementul Identității și Accesului: Pentru a schimba informații privind subiectele legate de Managementul Identității și Accesului.

Ambele părți sunt de acord să colaboreze și să facă schimb de informații în cadrul fiecăruia dintre procesele de securitate menționate mai sus. Părțile vor conveni asupra unor mijloace tehnice privind schimbul de informații în vederea asigurării conformității cu procedurile de securitate convenite.