C.N. ADMINISTRAȚIA PORTURILOR MARITIME S.A. Constanța
DIRECȚIA SECURITATE
DEPARTAMENTUL IT SI COMUNICAȚII
SERVICIUL COMUNICAȚII ȘI IT

APROBAT,
DIRECTOR SECURITATE
Ionuț Ducu POPESCU

AVIZAT,
ȘEF DEPARTAMENT IT ȘI COMUNICAȚII
Claudiu Cristinel GĂGĂUȚĂ

CAIET DE SARCINI
pentru achiziția
"CENTRALĂ TELEFONICĂ VOIP "

1 INTRODUCERE

Caietul de sarcini face parte integrantă din documentația de atribuire și constituie ansamblul cerințelor pe baza cărora se elaborează de către fiecare ofertant propunerea tehnică.

În cadrul acestei proceduri, Compania Națională „Administrația Porturilor Maritime" SA Constanța îndeplinește rolul de Autoritate/Entitate Contractantă, respectiv Autoritate/Entitate Contractantă în cadrul Contractului.

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.

Oferta tehnică va fi structurată exact ca specificația tehnică din Caietul de sarcini în scopul identificării caracteristicilor tehnice, conform solicitării Autorității Contractante.

Caracteristicile tehnice și cerințele din prezentul document constituie ansamblul cerințelor minime obligatorii pe baza cărora Ofertanții vor elabora propunerea tehnică și financiară.

Specificațiile tehnice care indică o anumită origine, sursă, producție, un procedeu special, o marcă de fabrică sau de comerț, un brevet de invenție, o licență de fabricație, sunt menționate doar pentru identificarea cu ușurință a tipului de produs și nu au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse.

Aceste specificații vor fi considerate ca având mențiunea de «sau echivalent» și vor fi considerate specificații minimale din punct de vedere al performanței, indiferent de marcă sau producător. Ofertantul trebuie să răspundă punctual la toate cerințele cuprinse în caietul de sarcini.

Ofertantul va desfășura activitățile, va realiza și furniza documentele/lucrările specifice contractului având în vedere toate prevederile legale naționale, europene și internaționale relevante existente la momentul semnării Contractului, precum și cele emise ulterior, pe parcursul derulării contractului, precum și ansamblul reglementărilor subsecvente, al recomandărilor și practicilor incidente.

Nu vor fi luate în considerare componente ale ofertei tehnice cum ar fi: pliante, diverse materiale promoționale ale firmelor producătoare sau furnizoare, prezentări, broșuri etc. care nu au legătură directă cu obiectul, structura și cerințele din prezentul Caiet de Sarcini.

2 CONTEXTUL REALIZĂRII ACESTEI ACHIZIȚII DE PRODUSE

2.1 Informații despre Autoritatea/entitatea contractantă

Compania "Administrația Porturilor Maritime" - S.A. Constanța este persoană juridică de naționalitate română, organizată ca societate pe acțiuni si funcționează sub autoritatea Ministerului Transporturilor și Infrastructurii și desfășoară activități de interes public național conform reglementărilor legale în vigoare și statutului.

3 DESCRIEREA PRODUSELOR SOLICITATE

Obiectul prezentei proceduri constă în achiziționarea următoarelor produse :

- Centrală telefonică VoIP (PBX)
- Session Border Controller (SBC)
- Terminale
- Servicii de migrare a actualei centrale
- Servicii de instalare și instruire pentru personal
- Servicii de garanție și update/upgrade

Configurațiile și cerințele tehnice minime obligatorii pe care trebuie să le îndeplinească produsele ofertate sunt prezentate în **Anexa 1 – Cerințe tehnice minime**.

4 CERINȚE DE GARANȚIE ȘI SUPORT TEHNIC PENTRU ECHIPAMENTELE LIVRATE

4.1 Toate echipamentele furnizate trebuie să fie noi și să beneficieze de o garanție de minim 24 de luni de la data livrării asigurate de producătorul acestora.

4.2 Nu se acceptă licențe refurbished sau remarketed. Licențele ofertate trebuie să fie noi – sigilate, canal distribuție oficial. Licențele vor putea fi înregistrate în conturile online ale autorității contractante.

4.3 Serviciile de garanție și suport tehnic pentru echipamente vor asigura înlocuirea oricărei componente, toate costurile înlocuirii legate de piese de schimb, manopera și orice alte cheltuieli asociate fiind suportate de către furnizorul produselor.

4.4 În perioada de garanție, serviciile de reparare / înlocuire se vor desfășura „on-site", fără deplasarea echipamentelor (posibilă doar în cazuri excepționale și doar cu aprobarea scrisă a beneficiarului).

4.5 În situația defectării unităților de stocare, acestea vor fi înlocuite fără a trimite către furnizor unitățile de stocare defecte. În situația în care este necesară trimiterea echipamentelor defecte la unitatea de Service Autorizată, ofertanții vor asigura transportul echipamentului.

4.6 Timpul de reparație: Maxim 30 de zile de la sesizarea adresată de către Achizitor.

5 LIVRARE, AMBALARE, ETICHETARE, TRANSPORT ȘI ASIGURARE PE DURATA TRANSPORTULUI

5.1 Produsele vor fi livrate cantitativ și calitativ la sediul CN APM SA Constanța.

5.2 Fiecare produs va fi însoțit de toate subansamblele / accesoriile / părțile componente necesare punerii și menținerii în funcțiune.

5.3 Termenul de livrare va fi de maxim 60 zile calendaristice de la data intrării în vigoare a contractului. Un produs este considerat livrat când toate activitățile din cadrul contractului au fost realizate și produsul / echipamentul este testat și funcționează la parametrii agreați și este acceptat de autoritatea contractantă.

5.4 Contractantul va informa Autoritatea Contractantă prin fax sau e-mail cu privire la data și ora de predare a produselor, cu cel puțin 2 zile lucrătoare, înainte de efectuarea acesteia.

5.5 Transportul și toate costurile asociate sunt în sarcina exclusivă a contractantului

5.6 Contractantul este responsabil pentru livrarea în termenul agreat al produselor și se consideră că a luat în considerare toate dificultățile pe care le-ar putea întâmpina în acest sens și nu va invoca niciun motiv de întârziere sau costuri suplimentare.

5.7 La livrare, produsele vor fi însoțite de următoarele documente:

a) Certificate de calitate și garanție de la producător, pentru fiecare echipament;
b) Aviz expediție
c) Licențe

6 RECEPȚIA PRODUSELOR

6.1 Recepția produselor se va efectua pe bază de proces verbal semnat de Contractant și Autoritatea Contractantă.

6.2 Recepția produselor constă în :

6.2.1 Recepția cantitativă (la livrarea echipamentelor) la sediul CN APM SA Constanța

6.2.2 Recepția calitativă (finală) după testarea echipamentelor și, după caz, toate defectele au fost remediate.

6.3 Autoritatea contractantă va efectua teste funcționale și de verificare a performanțelor tehnice solicitate ale produselor livrate, respectiv :

6.3.1 Verificarea performanțelor tehnice solicitate în caietul de sarcini

6.3.2 Instalarea și activarea produselor tip Office pe echipamentele livrate

6.4 După finalizarea testării se va întocmi Procesul verbal de recepție calitativă, ce va include unul din următoarele rezultate:

- acceptat
- acceptat cu observații minore
- acceptat cu rezerve
- refuzat

7 MODALITĂȚI DE PLATĂ

7.1 Contractantul va emite factura pentru produsele livrate prin e-factura. Factura va avea menționat numărul contractului, datele de emitere și scadența facturii respective.

7.2 Factura va fi emisă după semnarea de către Autoritatea contractantă a procesului verbal de recepție calitativă, acceptat, după livrare și testare.

7.3 Procesul verbal de recepție calitativă va însoți factura și reprezintă elementul necesar realizării plății, împreună cu celelalte documente justificative prevăzute mai jos:

a) Certificatul de calitate și garanție
b) Declarația de conformitate
e) Procesul verbal de recepție calitativă

7.4 Plățile în favoarea Contractantului se vor efectua în termen de 30 zile de la data emiterii facturii fiscale în original și a tuturor documentelor justificative.

8 FACTORI DE EVALUARE

a) Preț Total – 40 puncte.
b) HA/DR – timpi măsurați (RTO) + upgrade rolling - 25 puncte
c) Securitate – 20 puncte
d) Migrare, Garanție și suport – 15 puncte

Modalitate acordare punctaj

a) Pentru cel mai mic preț ofertat vor fi acordate 40 puncte. Pentru restul ofertelor, se va acorda punctajul după formula : P1= 40 x (Preț_minim / Preț_ofertat)
b) Cele 25 de puncte pentru HA/DR – timpi măsurați (RTO) + upgrade rolling vor fi acordate astfel :
   - RTO failover SBC (10 puncte)

     RTO = timp până la reluarea funcționării serviciului după căderea nodului activ.

     Punctajul va fi acordat astfel :

     10 p: RTO ≤ 30 sec

     7 p: 31–60 sec

     4 p: 61–120 sec

     0 p: >120 sec

     Ofertanții vor face dovada conformității prin depunerea documentației tehnice oficiale a producătorului (datasheet/manual/catalog), din care să rezulte în mod explicit specificațiile ofertate, indicând în clar pentru fiecare cerință pagina, capitolul/ secțiunea și, după caz, paragraful/tabelul/figura unde se regăsește informația.

- RTO failover PBX/registrar (10 p)
  Punctajul va fi acordat astfel :
  10 p: RTO ≤ 60 sec
  7 p: 61–120 sec
  4 p: 121–300 sec
  0 p: >300 sec (idem ca mai sus)
  Ofertanții vor face dovada conformității prin depunerea documentației tehnice oficiale a producătorului (datasheet/manual/catalog), din care să rezulte în mod explicit specificațiile ofertate, indicând în clar pentru fiecare cerință pagina, capitolul/ secțiunea și, după caz, paragraful/tabelul/figura unde se regăsește informația.
- Upgrade „rolling" fără întrerupere semnificativă
  5p: upgrade rolling pentru SBC + PBX (fără întrerupere percepută > 60 sec la nivel de servicii critice) + procedură
  3 p: upgrade rolling doar pentru SBC (conform minimului) + procedură
  0 p: nu demonstrează rolling / doar downtime clasic
  Ofertanții vor face dovada conformității prin depunerea documentației tehnice oficiale a producătorului (datasheet/manual/catalog), din care să rezulte în mod explicit specificațiile ofertate, indicând în clar pentru fiecare cerință pagina, capitolul/ secțiunea și, după caz, paragraful/tabelul/figura unde se regăsește informația.

c) Securitate – 20 puncte

C1. FIPS (6 p)

- 6 p: suport FIPS 140-2/140-3 (mod FIPS disponibil) + document oficial producător
- 0 p: nu are

Ofertanții vor face dovada conformității prin depunerea documentației tehnice oficiale a producătorului (datasheet/manual/catalog), din care să rezulte în mod explicit specificațiile ofertate, indicând în clar pentru fiecare cerință pagina, capitolul/ secțiunea și, după caz, paragraful/tabelul/figura unde se regăsește informația.

Ofertanții au obligația de a prezenta documentația tehnică a producătorului, cu indicarea expresă a conformității cu cerințele stabilite prin prezentul caiet de sarcini și cu precizarea clară a capitolului, paginii sau paragrafului din documentație, necesare pentru evaluare și stabilirea punctajului.

C2. Loguri „tamper-proof" cu WORM / log signing + retenție (7 p)

- 7 p: log signing și export către storage WORM / immutable (sau echivalent demonstrat) + configurare retenție
- 3 p: log signing sau WORM (doar una)
- 0 p: doar loguri standard

Ofertanții vor face dovada conformității prin depunerea documentației tehnice oficiale a producătorului (datasheet/manual/catalog), din care să rezulte în mod explicit specificațiile ofertate, indicând în clar pentru fiecare cerință pagina, capitolul/ secțiunea și, după caz, paragraful/tabelul/figura unde se regăsește informația.

Ofertanții au obligația de a demonstra îndeplinirea cerințelor prin prezentarea manualelor aferente, a capturilor de ecran din configurare și a descrierii detaliate a arhitecturii soluției. Neprezentarea, prezentarea incompletă sau lipsa indicării elementelor relevante din aceste documente conduce la neacordarea punctajului aferent criteriilor de evaluare.

C3. TLS 1.3 nativ + politici cipher (7 p)

- 7 p: TLS 1.3 nativ + configurare explicită cipher suites + PFS demonstrat (ECDHE)
- 3 p: TLS 1.3 nativ, dar fără control granular (sau limitat)
- 0 p: TLS 1.2 only (cu/ fără justificare) – rămâne conform dacă minimul permite

Ofertanții au obligația de a demonstra îndeplinirea cerințelor de securitate prin prezentarea Security Guide-ului producătorului și a documentației de configurare, cu indicarea explicită a elementelor relevante; neprezentarea sau prezentarea incompletă conduce la neacordarea punctajului aferent.

d) Migrare, Garanție și suport – 15 puncte

D1. Migrare și downtime – 5 puncte

Downtime și rollback mai mic sau egal cu 60 minute – 5 puncte
Downtime și rollback mai mare de 60 minute – 0 puncte
Dovada : plan migrare cu pași și ferestre, plan rollback

D2. Garanție – 5 puncte
Perioada de Garanție mai mare sau egală cu 36 luni – 5 puncte
Perioada de Garanție cuprinsă între 25 și 35 luni – 2 puncte
Perioada de Garanție – 24 de luni – Cerință minimă obligatorie – 0 puncte

D3. Timp reparații – 5 puncte
Timp de raparație mai mic sau egal cu 48 ore – 5 puncte
Timp de reparație cuprins între 48 ore și 96 ore – 2 puncte
Timp mai mare de 96 ore – 0 puncte.

În cazul în care nu este respectat SLA-ul ofertat, se vor percepe penalități în valoare de 1000 RON / 24 ore întarziere. Penalitățile vor fi calculate începând cu prima oră de depășire a SLA-ului.
(Exemplu: Se ofertează SLA de maxim 48 ore. Dacă problema este soluționată în 49 de ore, sau orice interval până la 72 ore – se percep penalități de 1000 lei. Dacă problema este soluționată în 73 ore – se percep penalități de 2000 RON).

Șef Serviciu Comunicații și IT
cu atribuții delegate
Iustin OBREJA

Întocmit
Ionuț TODE

Anexa 1 – Cerinte tehnice minime

Nr. Crt.	Cerințe minime obligatorii pentru arhitectură, topologie și compatibilitate
1.	Soluția va implementa modelul IP-PBX + SBC/secure edge pentru acces remote al telefoanelor IP.
2.	Soluția va permite înregistrarea telefoanelor IP din Internet către PBX prin SBC, fără expunerea directă a PBX-ului în Internet.
3.	Soluția va furniza topologie recomandată DMZ (SBC în DMZ, PBX în LAN) ca implementare standard. Vor fi acceptate si alte soluții considerate echivalente.
4.	Soluția va fi implementata on-prem pentru PBX.
5.	Soluția va suporta SBC ca appliance sau VM sau container (minimum una, documentat).
6.	Soluția va asigura funcționarea cu NAT pentru endpoint-uri remote.
7.	Soluția va asigura funcționarea cu double NAT pentru endpoint-uri remote.
8.	Soluția va asigura funcționarea în medii CGNAT pentru endpoint-uri remote.
9.	Soluția va suporta IPv4 integral.
10.	Soluția va suporta dual-stack IPv4/IPv6 sau se vor documenta explicit limitările (fără a afecta funcționarea IPv4).
11.	Soluția va permite definirea a minimum 1000 endpoint-uri per instanță (sau scalare echivalentă documentată).
12.	Ofertantii vor furniza metodologie de dimensionare pentru număr de înregistrări simultane (concurrent registrations).
13.	Ofertantii vor furniza metodologie de dimensionare pentru apeluri simultane (concurrent calls).
14.	Ofertantii vor furniza metodologie de dimensionare pentru BHCA.
15.	Ofertantii vor furniza lista completă de porturi/protocoale (signaling, media, provisioning, management).
16.	Soluția va suporta operare multi-site (minimum 2 locații) în același dial-plan.
17.	Soluția va suporta plan de numerotație cu extensii + normalizare E.164.
18.	**Soluția va suporta minimum 11 SIP trunk-uri simultan.**
19.	Soluția va suporta failover trunk între minimum 2 furnizori/carrieri.
20.	Soluția va suporta DNS SRV/NAPTR pentru rezoluție și redundanță
21.	Soluția va permite separarea planului de management de planul de semnalizare/media (segmentare).
22.	Ofertantii vor documenta cerințe NTP și comportamentul la drift.
23.	Soluția va suporta integrare LDAP/AD pentru director (minimum import utilizatori).
24.	Soluția va permite politici diferite per site (remote vs office).
25.	Ofertantii vor furniza un ghid de compatibilitate pentru routere casnice (SIP ALG, NAT keepalive).
26.	**Cerințe minime obligatorii pentru SBC – funcții SIP și media**
27.	SBC va opera stateful și va furniza control complet dialog SIP (B2BUA sau echivalent).
28.	Soluția va implementa topology hiding (mascare IP/headers interne).
29.	Soluția va implementa normalizare/manipulare de headere SIP și SDP (rewrite Contact/Via/SDP).
30.	Soluția va ancora media prin RTP relay/anchoring pentru endpoint-uri remote.
31.	Soluția va gestiona NAT traversal pentru signaling și media.
32.	Soluția va suporta SIP over TLS.
33.	Soluția va suporta SRTP.
34.	Soluția va permite impunerea TLS obligatoriu pentru telefoane remote.
35.	Soluția va permite impunerea SRTP obligatoriu pentru telefoane remote.
36.	Soluția va suporta SIP over TCP.
37.	Soluția va suporta SIP over UDP (interop), cu posibilitate de restricționare pe WAN.
38.	Soluția va suporta OPTIONS keepalive configurabil.
39.	Soluția va suporta tuning pentru registration keepalive/NAT keepalive.
40.	Soluția va suporta SIP Session Timers.
41.	Soluția va suporta re-INVITE (hold/resume).

42.	Soluția va suporta UPDATE (unde e cazul).
43.	Soluția va gestiona early media corect.
44.	Soluția va suporta PRACK (100rel) sau profil explicit de interop (fără pierdere funcțională).
45.	Soluția va suporta SIP REFER (transfer) cu politici.
46.	Soluția va păstra corect Diversion/History-Info pentru redirecționări.
47.	Soluția va gestiona P-Asserted-Identity și privacy policy.
48.	Soluția va suporta DTMF RFC2833/4733.
49.	Soluția va suporta DTMF prin SIP INFO (passthrough unde e necesar).
50.	Soluția va suporta policy de codec per grup (remote vs intern).
51.	Soluția va asigura end-to-end minimum G.711; transcoding este acceptat dacă este disponibil și documentat.
52.	Soluția va suporta G.711.
53.	Soluția va suporta G.722 sau echivalent wideband.
54.	Soluția va suporta Opus sau alternativă echivalentă demonstrată fără degradare neacceptabilă (în caz contrar, neeligibil).
55.	Soluția va permite controlul RTP port range.
56.	Soluția va permite whitelist de metode SIP acceptate.
57.	Soluția va aplica SIP sanity checks (SDP invalid, headere malformate).
58.	Soluția va gestiona robust dimensiunea mesajelor SIP și anomalii.
59.	Soluția va suporta failover DNS între noduri PBX/registrar.
60.	Soluția va suporta load balancing către multiple noduri PBX (unde există cluster).
61.	Soluția va implementa health checks și failover automat către PBX nodes.
62.	Soluția va separa politici pentru remote vs trunk.
63.	Soluția va implementa media policing (anti RTP flood).
64.	Soluția va implementa rate limits pentru REGISTER/INVITE.
65.	Soluția va implementa blocklist dinamic.
66.	Soluția va implementa protecții DoS la nivel SIP.
67.	Soluția va permite restricții geo-IP (allow/deny pe țări).
68.	Soluția va permite allow/deny lists pe IP/subnet.
69.	Soluția va asigura mascarea IP-urilor interne în SDP în toate scenariile.
70.	Soluția va asigura management complet certificate TLS (import, chain, renew).
71.	Soluția va furniza interop documentat cu minimum 2 producători majori de telefoane SIP.
72.	**Cerințe minime obligatorii pentru provisioning, zero-touch și lifecycle device**
73.	Soluția va asigura zero-touch provisioning pentru minimum un vendor major; Soluția va lista exact modelele/seriile suportate.
74.	Provisioning-ul se va realiza prin HTTPS.
75.	Soluția va utiliza șabloane (templates) per model și per grup.
76.	Soluția va permite provisioning per device (MAC).
77.	Soluția va permite provisioning per user (mapare user-device).
78.	Soluția va permite bulk import (CSV/API) pentru utilizatori și device-uri.
79.	Soluția va asigura onboarding securizat prin activation code sau metodă echivalentă.
80.	Soluția va separa credențialele SIP registration de credențialele admin/provisioning.
81.	Soluția va permite rotația credențialelor la scară (bulk).
82.	Soluția va permite carantinarea device-urilor până la aprobare.
83.	Soluția va permite tagging (site/department/cost center).
84.	Soluția va permite hot-desking/extension mobility (login user pe alt telefon).
85.	Soluția va permite multi-device per user (desk + softphone) cu politici.
86.	Soluția va furniza inventory endpoint (model, MAC/serial, firmware, last seen).
87.	Soluția va furniza management firmware (minimum recomandare + validare versiuni).

88.	Soluția va permite lockdown (dezactivare acces local web UI sau control acces).
89.	Soluția va permite PIN protecție pentru meniuri și acțiuni critice.
90.	Soluția va detecta și raporta config drift.
91.	Soluția va asigura proces rapid pentru RMA replacement (swap device).
92.	Soluția va furniza status endpoint (registered/unregistered + cauză eșec).
93.	Soluția va furniza audit log pentru provisioning (cine/ce/când).
94.	Soluția va permite staged rollout și rollback config.
95.	Soluția va configura time zone per user/device.
96.	Soluția va configura language/locale per user/device.
97.	Soluția va configura DSCP/QoS per endpoint și/sau SBC.
98.	Soluția va furniza procedură ship-to-home (preprovision + plug-and-play).
99.	Soluția va furniza recomandări și setări pentru mitigarea SIP ALG.
100.	Soluția va configura intervale NAT keepalive per profil.
101.	Soluția va furniza diagnostic la distanță (colectare loguri endpoint).
102.	Soluția va furniza SIP trace per call-id (PBX/SBC).
103.	Soluția va furniza PCAP capture la nivel SBC cu control acces.
104.	Soluția va permite export securizat al capturilor și retenție configurabilă.
105.	Soluția va monitoriza "endpoint movement" (schimbare IP/ASN/țară).
106.	Soluția va genera alertă la schimbare țară (configurabil).
107.	Onboarding-ul se va realiza fără prezență fizică IT la utilizator.
108.	Soluția va documenta limitele suportate (endpoint-uri, concurrency).
109.	Soluția va furniza matrix de interoperabilitate (model + firmware + caveats).
110.	Se vor defini profiluri dedicate pentru remote phones.
111.	Se vor defini profiluri dedicate pentru office LAN phones.
112.	Se vor defini profiluri dedicate pentru common area phones.
113.	Soluția va furniza procedură factory reset + reprovision.
114.	Soluția va furniza mecanism de revocare device (blocare registrare).
115.	Soluția va furniza raport de compliance endpoint (firmware minim, TLS/SRTP).
116.	Soluția va impune firmware minim per model (unde este suportat).
117.	Se vor impune setări minime de securitate per profil endpoint.
118.	**Cerințe minime obligatorii pentru identitate, autentificare, RBAC și SSO**
119.	Soluția va utiliza credențiale unice per user/device (fără parole partajate).
120.	Soluția va impune politici de parolă (lungime, complexitate).
121.	Soluția va aplica lockout după încercări eșuate (configurabil).
122.	Soluția va aplica protecții brute-force pe registration.
123.	Soluția va implementa RBAC granular (minim admin, helpdesk, auditor).
124.	Soluția va asigura segregare per site a administratorilor (scope).
125.	Soluția va menține audit trail pentru acțiuni administrative.
126.	Soluția va asigura MFA pentru acces administrativ (TOTP sau echivalent).
127.	Soluția va permite impunerea obligatorie a MFA.
128.	Soluția va suporta SSO pentru portaluri (SAML2 sau OIDC).
129.	Soluția va suporta integrare AD/LDAP pentru autentificare sau sincronizare.
130.	Soluția va suporta SCIM sau mecanism echivalent de lifecycle user (create/disable).
131.	Soluția va utiliza API keys cu scope și rotație.
132.	Soluția va restricționa accesul la admin portal pe IP (configurabil).
133.	Soluția va configura session timeout pentru portal.
134.	Soluția va furniza cont break-glass cu audit și alert.
135.	Soluția va aplica politici per user pentru internațional/premium/mobil.
136.	Soluția va aplica politici per device pentru permisiuni apel.

137.	Soluția va implementa măsuri anti toll-fraud (mecanisme + recomandări).
138.	Soluția va implementa detecție anomalii pentru volum/destinații.
139.	Soluția va genera alerte pentru spike de cost/trafic.
140.	Soluția va valida caller ID (prevenire spoof intern).
141.	Soluția va aplica politici de privacy (CLIR/anonymous) controlate.
142.	Soluția va documenta suportul STIR/SHAKEN (dacă este relevant).
143.	Soluția va aplica politici time-of-day pentru apeluri.
144.	Soluția va aplica politici geo-fencing pentru registrations/calls.
145.	Soluția va aplica restricții pe ASN (dacă disponibil) sau echivalent.
146.	Soluția va aplica limitări de rată/număr apeluri per interval per user.
147.	Soluția va aplica limitări de rată per device.
148.	Soluția va permite mecanism "four-eyes" pentru schimbări critice sau echivalent.
149.	Rolul auditor va avea acces read-only la loguri și configurații relevante.
150.	Soluția va aplica mascarea PII în loguri (configurabil).
151.	Soluția va controla exportul secretelor (interzis sau strict controlat).
152.	Soluția va documenta protecția credențialelor/cheilor (storage, hashing, acces).
153.	Soluția va integra cu vault/KMS sau se va livra alternativă echivalentă documentată.
154.	Soluția va permite rotația certificatelor fără downtime semnificativ.
155.	Dezactivarea unui utilizator va revoca accesul rapid (disable).
156.	Propagarea dezactivării către acces remote se va realiza în maximum 5 minute (documentat).
157.	Soluția va furniza raport RBAC complet (cine are ce drepturi).
158.	Soluția va exporta audit log către SIEM.
159.	**Cerințe minime obligatorii pentru criptografie, hardening și protecții**
160.	Soluția va suporta minimum TLS 1.2.
161.	Soluția va permite dezactivarea TLS sub 1.2.
162.	Soluția va suporta TLS 1.3 sau se va livra justificare tehnică fără impact asupra securității minime; se vor utiliza cipher-uri PFS.
163.	Soluția va permite configurarea cipher suites.
164.	Soluția va utiliza suite cu Perfect Forward Secrecy (ECDHE).
165.	Soluția va asigura management complet de certificate (chain/intermediate/root).
166.	Soluția va suporta SRTP cu suite standard documentate.
167.	Soluția va impune SRTP "required" per profil (remote).
168.	Soluția va impune TLS "required" per profil (remote).
169.	Soluția va implementa protecții anti SIP scan (drop/tarpit/block).
170.	Soluția va implementa protecții anti REGISTER flood.
171.	Soluția va implementa protecții anti INVITE flood.
172.	Soluția va implementa protecții anti credential-stuffing.
173.	Soluția va configura rate limits per IP.
174.	Soluția va configura rate limits per user/extension.
175.	Soluția va administra blocklist temporar și permanent.
176.	Soluția va administra allowlist prioritar.
177.	Soluția va exporta evenimente către syslog.
178.	Soluția va furniza integrare SIEM (format documentat).
179.	Soluția va separa management plane cu interfețe dedicate.
180.	Soluția va permite autentificare management cu chei SSH (unde se aplică).
181.	Soluția va dezactiva servicii nefolosite (hardening).
182.	Soluția va livra ghid oficial de hardening.
183.	Soluția va livra politică de patching și management vulnerabilități.
184.	Furnizorul va avea proces documentat de advisories (public/privat).

185.	Soluția va cripta "at rest" baza de date/config (platformă).
186.	Se vor cripta backup-urile.
187.	Soluția va configura retenția backup-urilor.
188.	Soluția va permite rotația cheilor de criptare sau procedură echivalentă.
189.	Audit logs vor fi tamper-resistant (log signing sau export write-once).
190.	Soluția va configura retenția audit logs.
191.	Soluția va permite minimizarea PII în loguri.
192.	Se vor asigura controale GDPR aplicabile (export/ștergere unde e cazul).
193.	PBX-ul nu va fi expus direct în Internet pentru registrări remote.
194.	Soluția va documenta mecanismul exact "no direct SIP to PBX".
195.	Soluția va implementa whitelist metode SIP permise.
196.	Soluția va valida SDP pentru prevenirea leak de IP intern.
197.	Soluția va permite trunk securizat (TLS către carrier dacă suportat).
198.	Soluția va aplica restricții pe destinații (premium/international) la nivel de politică.
199.	Soluția va aplica protecții anti-fraud pentru destinații cu risc.
200.	Soluția va genera alerte pentru modificări critice de configurație.
201.	Soluția va genera alerte pentru autentificări admin suspecte.
202.	Soluția va genera alerte pentru endpoint nou/necunoscut.
203.	Soluția va suporta modul FIPS dacă este cerut explicit în RFP (în lipsă, se declară suportul/ne-suportul, dar cerința rămâne eliminatorie dacă e solicitată).
204.	Soluția va furniza recomandări de segmentare VLAN și reguli firewall.
205.	**Cerințe minime obligatorii pentru disponibilitate, HA, DR și upgrade (201–230)**
206.	Soluția va implementa SBC HA (active/standby) cu failover automat.
207.	Soluția va asigura sincronizare de stare pentru failover (minim registrări; apeluri unde este posibil).
208.	Soluția va asigura redundanță PBX (cluster/HA minim 2 noduri sau echivalent documentat).
209.	Soluția va asigura failover pentru endpoint-uri remote între minimum 2 SBC-uri.
210.	Soluția va asigura failover prin DNS SRV sau VIP.
211.	Soluția va controla re-registrările în masă (anti thundering herd).
212.	Soluția va aplica rate limits pentru re-registrări post-outage.
213.	Soluția va realiza backup complet PBX + SBC (config + policies).
214.	Soluția va realiza backup programat.
215.	Soluția va furniza procedură de restore testată.
216.	Se vor defini RTO/RPO recomandate și pașii DR.
217.	Soluția va furniza procedură de upgrade cu downtime minim.
218.	Soluția va furniza procedură de rollback versiune/config.
219.	Soluția va permite "drain" de nod pentru mentenanță.
220.	Soluția va permite upgrade rolling la nivel de SBC HA (minim).
221.	Soluția va permite scalare orizontală prin adăugare noduri SBC.
222.	Soluția va documenta licențierea în HA (pooling/per node).
223.	Soluția va preveni split-brain în HA.
224.	Soluția va furniza monitorizare health pentru noduri și servicii.
225.	Soluția va furniza monitorizare health pentru trunk-uri.
226.	Soluția va furniza monitorizare health pentru media relay.
227.	Soluția va furniza monitorizare WAN/link și impact asupra rutării.
228.	Soluția va documenta survivability pentru apeluri interne la cădere WAN (și implementarea dacă este cerută).
229.	Se vor documenta politicile pentru apeluri de urgență și funcționarea în scenarii de degradare.
230.	Soluția va furniza plan de testare HA/DR pentru acceptanță.
231.	Soluția va furniza rapoarte de disponibilitate.

232.	Soluția va furniza SLA suport (timp răspuns/incidente).
233.	Soluția va furniza SLA patch-uri de securitate (timp publicare/fix).
234.	Soluția va furniza guidance pentru ferestre de mentenanță.
235.	Soluția va furniza politici EOL/EOS și versiuni suportate.
236.	**Cerințe minime obligatorii pentru calitate voce, QoS, metrici și troubleshooting**
237.	Soluția va colecta statistici RTP/RTCP per apel.
238.	Soluția va afișa indicatori de calitate (jitter, loss, RTT).
239.	Soluția va calcula/estima MOS (sau metric echivalent) și se vor permite praguri de alertare.
240.	Soluția va genera alerte pentru degradare calitate (MOS/jitter/loss).
241.	Soluția va aplica DSCP markings pentru SIP și RTP pe SBC.
242.	Soluția va păstra sau reasigna QoS markings (documentat).
243.	Soluția va aplica politici codec dedicate pentru remote (optimizare bandwidth).
244.	Soluția va documenta consumul de bandă per codec și concurrency.
245.	Soluția va aplica call admission control (CAC) sau mecanism echivalent.
246.	Soluția va asigura DTMF fiabil pentru IVR-uri (plan de test inclus).
247.	Soluția va asigura transferurile blind/attended end-to-end pentru remote.
248.	Soluția va asigura voicemail și MWI pentru remote.
249.	Soluția va asigura conferințe (minim 3 participanți) cu remote.
250.	Soluția va furniza CDR complete (orig/dest, duration, cause codes).
251.	Soluția va furniza cause codes detaliate pentru eșecuri apel/registrare.
252.	Soluția va furniza SIP ladder/trace per call-id din UI sau CLI.
253.	Soluția va furniza PCAP per endpoint/call la nivel SBC.
254.	Soluția va permite export CDR către sisteme externe (CSV/API).
255.	Soluția va suporta SNMP și/sau Prometheus (minimum una).
256.	Soluția va exporta syslog către SIEM și se va asigura corelarea evenimentelor (ID-uri consistente).
257.	**Cerințe minime obligatorii pentru migrare în paralel și cutover cu downtime cumulat max. 2 ore**
258.	Furnizorul va livra plan complet de migrare (faze, dependențe, riscuri, rollback) înainte de implementare.
259.	Furnizorul va livra plan de coexistență (funcționare paralelă) pe perioada agreată (minimum 14 zile sau conform beneficiar).
260.	Migrarea se va realiza etapizat (departamente/grupuri/locații/intervale extensii), fără întrerupere pentru restul utilizatorilor.
261.	Soluția va asigura funcționarea în paralel cu rutare bidirecțională între PBX vechi și PBX nou (inter-PBX).
262.	Soluția va asigura apelare internă între extensii aflate pe vechi și pe nou (dial-plan integrat).
263.	Se va asigura transfer blind între PBX-uri în ambele direcții.
264.	Se va asigura transfer attended între PBX-uri în ambele direcții.
265.	Se va asigura hold/resume fără defecte în scenariu cross-PBX.
266.	Soluția va asigura conferințe în scenariu mixt (participanți vechi + nou) fără degradare majoră.
267.	Se va asigura voicemail/MWI coerent în scenariu mixt (documentat).
268.	Furnizorul va implementa SIP peering între centrale (SIP trunk inter-PBX) securizat (TLS/SRTP unde este posibil).
269.	Inter-PBX va include normalizare numerotație și mapare extensii (intern ↔ E.164).
270.	Inter-PBX va păstra CLI/ANI corect în ambele direcții.
271.	Inter-PBX va gestiona Diversion/History-Info sau echivalent pentru forward.
272.	Furnizorul va furniza plan de test interop inter-PBX (DTMF, early media, transfer, fax dacă există).
273.	Se vor păstra numerele DID existente fără renumerotare (exceptând cazuri aprobate în scris).
274.	Se vor păstra extensiile existente pentru minimum 95% dintre utilizatori.
275.	Se vor păstra grupurile de apel (hunt/ring groups) cu aceeași logică.
276.	Se vor păstra IVR-urile (meniuri, mesaje, rute).
277.	Se vor păstra programele de lucru și rutele aferente.

278.	Se vor păstra regulile de forward (CFU/CFB/CFNR) prin import automat/semi-automat.
279.	Se vor păstra blacklist/whitelist și politicile anti-fraud
280.	Se vor păstra codurile de cost/departamente și rapoartele aferente (dacă există).
281.	Furnizorul va realiza inventarierea completă a centralei existente înainte de cutover.
282.	Furnizorul va produce document As-Is și To-Be cu diferențe și justificări.
283.	Furnizorul va identifica și documenta toate integrările (trunk, recording, CRM, paging, interfoane, fax, contact center etc.).
284.	Planul va include dependențe externe (carrier, DNS, certificate, firewall).
285.	Furnizorul va furniza lista completă de schimbări firewall și impact înainte de implementare.
286.	Soluția va utiliza dual registration sau mecanism echivalent pe perioada de tranziție, unde este tehnic posibil.
287.	Pentru modele fără dual registration se va asigura reprovisioning rapid (sub 5 minute/telefon) și validare.
288.	Soluția va asigura mass provisioning cu rollback la config veche în < 15 minute pe lot.
289.	Telefoanele remote se vor migra fără deplasare fizică și fără întrerupere > 10 minute per utilizator.
290.	Telefoanele interne se vor migra pe loturi fără întrerupere > 10 minute per utilizator.
291.	Downtime-ul cumulat al cutover-ului va fi maximum 2 ore (definit ca indisponibilitate inițiere/primire apeluri).
292.	Strategia de cutover va ținti downtime ≤ 30 minute.
293.	Cutover-ul va fi planificat în fereastră de mentenanță agreată cu notificare către utilizatori, preferabil in weekend.
294.	**Furnizorul va furniza plan de rollback executabil în maximum 60 minute.**
295.	Rollback-ul va fi demonstrat în pre-producție înainte de cutover final.
296.	Planul va include criterii Go/No-Go înainte de comutare.
297.	Planul va include criterii de acceptanță post-cutover (intern, extern, inbound/outbound, transfer, IVR, voicemail, conferință).
298.	În coexistență Soluția va permite rutare inbound DID către vechi sau nou pe procente/intervale (traffic steering).
299.	În coexistență Soluția va permite rutare outbound controlată (LCR comun sau separare controlată).
300.	Mutarea inbound pentru un DID de pe vechi pe nou și înapoi se va realiza în < 10 minute (carrier/SBC, documentat).
301.	Mutarea unui grup de DIDs se va realiza în loturi fără downtime major.
302.	Metoda de DID cutover (portare/redirecționare carrier/trunk swapping/număr virtual) va fi definită în scris cu impact pe downtime.
303.	Soluția va asigura sincronizare director (AD/LDAP) astfel încât utilizatorii să existe pe nou înainte de migrare.
304.	Importul utilizatorilor va include atribute: nume, extensie, DID, departament, politici.
305.	Politicile de apelare (internațional/premium) vor fi identice sau mai restrictive decât pe vechi.
306.	Nu se va produce escaladare de privilegii după migrare.
307.	Înregistrările de apel (dacă există) vor fi migrate sau se va asigura acces continuu la arhiva veche pe perioada legală.
308.	Furnizorul va implementa mediu staging/pre-producție cu minimum 20% din configurația reală.
309.	Se vor executa teste de acceptanță în staging: inbound/outbound, IVR, transfer, DTMF, TLS/SRTP, failover.
310.	Se va executa test de încărcare la minimum 30% din concurrency target.
311.	Se va executa test failover HA (SBC și PBX) înainte de producție.
312.	Se va executa test de apeluri remote din minimum 5 locații/ISP-uri diferite înainte de producție.
313.	În timpul migrarii se va asigura monitorizare în timp real (registrations, CSR, MOS/jitter/loss).
314.	Se va organiza "war room" operațional pe durata cutover-ului (telephony, network, security).
315.	Furnizorul va furniza escaladare și contacte 24/7 în fereastra de migrare.

316.	Furnizorul va furniza raport post-migrare (migrat, excepții, ce rămâne pe vechi).
317.	În coexistență se va asigura CDR unificat sau agregare într-o platformă comună de raportare.
318.	Se va asigura corelare apeluri între PBX-uri (call-id mapping sau echivalent).
319.	Se vor păstra cause codes și motivele eșecurilor în ambele platforme.
320.	Integrările critice vor funcționa înainte de cutover final (recording, paging, interfoane etc., după caz).
321.	Pentru integrări non-critice se va asigura workaround temporar fără blocarea migrarei.
322.	Orice deviație de la As-Is va fi documentată și acceptată în scris.
323.	În coexistență nu se va introduce niciun single point of failure nou (SBC redundant, PBX redundant, trunk redundant).
324.	Se va furniza plan de back-out pentru orice schimbare firewall/DNS/certificate.
325.	Furnizorul va livra training minim pentru helpdesk înainte de cutover.
326.	Furnizorul va livra ghid de utilizator pentru remote phone + proceduri self-check.
327.	Furnizorul va livra checklist pentru utilizatori înainte de comutare (power cycle, cablare, internet).
328.	Contractual, downtime cumulat > 2 ore va constitui neconformitate si se vor percepe penalitati in valoare de 1% din totalul contractului pentru fiecare ora.
329.	Se vor asuma indicatori post-cutover: call completion rate ≥ 99% în primele 48h (sau prag agreat).
330.	Se vor asuma indicatori post-cutover: registration success rate ≥ 99% pentru endpoint-uri active.
331.	Defectele critice în primele 72h vor fi remediate în < 4 ore (sau SLA agreat).
332.	**Se va asigura suport dedicat (on-site sau remote) în primele 10 zile lucrătoare post-cutover, post migrare utilizatori. Capacitatea de migrare a terminalelor/utilizatorilor a Entitatii Contractante este de minim 10 maxim 20 terminale pe ora.**
333.	Centrala veche va rămâne în stare de readiness până la acceptanța finală semnată.
334.	Se va defini un freeze window înainte de cutover (fără schimbări pe vechi, cu excepții controlate).
335.	Configurația finală de pe vechea centrală va fi exportată pentru arhivare (dacă este posibil).
336.	Furnizorul va livra documentație as-built pentru soluția nouă după stabilizare.
337.	Funcționarea în paralel și cutover în limita de downtime se vor demonstra prin test de acceptanță executat și semnat.
338.	Vor fi acceptate si alte scenarii de migrare, echivalente, pentru care downtime-ul global nu depaseste 2 ore. Ofertantii vor prezenta in detaliu metodologia de migrare si se vor incadra in downtime de maximum 2 ore. Entitatea Contractanta propune 2 strategii pentru migrare, dar vor fi acceptate si alte strategii ale furnizorului, daca acestea respecta termenjul de 2 ore de downtime. Strategiile propuse pentru respectarea termenului de downtime sunt: a)Pastrare PRI-uri initiale + Media Gateway E1/PRI ↔ SIP spre noul PBX si eventual si spre vechiul PBX astfel incat sa se poata face steering si coexistenta (varianta preferata de Entitatea contractanta, fiind cea mai sigura din punct de Vedere operational); b)Migrarea Trunks la SIP (carrier) + DID steering gradual catre noul PBX , pastrand vechiul PBX interconectat prin SIP peering pana sunt migrate toate extensiile. (Varianta fezabila pentru un downtime de 2 ore dar dependenta de carrier). Vor fi acceptate si alte scenarii propuse daca acestea se incadreaza in downtime de maximum 2 ore. Nota : Downtime-ul local, per utilizator, la migrarea catre noul terminal, nu va fi contorizat. Downtime-ul GLOBAL, per PBX/SBC, va fi contorizat si nu trebuie sa depaseasca 2 ore.
339.	Solutia va avea posibilitatea de înregsitrare a conținutului convorbirilor telefonice.
340.	Furnizorul va livra :
341.	Terminale fara fir, tip DECT, VoIP - 780 bucăți. Acestea vor putea fi provizionate din orice retea wireless, vor fi usor de configurat si vor putea salva minim 5 retele wireless, fara a necesita reconfigurarea.
342.	terminale VoIP tip 1(facilități de bază) - 150 bucăți.
343.	terminale VoIP tip 2(facilități medii) - 60 bucăți.

344.	terminale VoIP tip3(facilități avansate) - 60 bucăți.
345.	Soluția va prevedea toate operațiunile de mutare/relocare/instalare pentru toate echipamentele ce deservesc serviciile de voce solicitate prin acest caiet de sarcini.

1. ȘCOLARIZARE

Instruirile și școlarizările se vor efectua în România. Costurile vor fi suportate de către contractant.

Sculele, echipamentul de lucru și materialele necesare pentru programul de școlarizare vor fi puse la dispoziție de către contractant.

Stabilirea duratei de pregătire a personalului cade în sarcina contractantului, dar nu va fi mai mică de 5 zile, astfel încât la sfârșitul perioadei de școlarizare, cursanții vor fi capabili să realizeze singuri operarea, întreținerea și depanarea echipamentului, în condiții de acuratețe care să nu afecteze durata de viață a utilajului/echipamentului respectiv, așa cum este ea garantată de antreprenor.

Se vor prelucra minim următoarele:

- Cunoștințe generale asupra sistemului telefonic, componente și funcții de bază
- Funcții avansate
- Programare și configurare Centrală telefonică(PBX+SBC) și aparate telefonice
- Monitorizare și administrare. Utilizare aplicații software management, contorizare convorbiri, alarme, etc.
- Întreținere și mentenanță
- Cunoștințe particulare asupra sistemului telefonic care va fi instalat.

2. ASIGURAREA DOCUMENTAȚIEI TEHNICE PENTRU OPERARE ȘI MENTENANȚĂ

În sarcina Furnizorului cade asigurarea manualelor de operare și mentenanță necesare pentru personalul de supraveghere, de exploatare sau alt personal tehnic al Beneficiarului.Fiecare manual va fi împărțit în secțiuni indexate logic. Acestea vor de preferință în format A4 și vor fi rezistente la uzură.

MANUALUL PENTRU OPERARE

Furnizorul va pune la dispoziția Beneficiarului manuale de operare care sa explice scopul și funcționarea întregului sistem, împreună cu manuale pentru subsistemele lui componente și pentru echipamente individuale. Pentru echipamente și subsisteme vor fi furnizate manuale care să conțină caracteristicile tehnice și limitele de operare (dacă este cazul).

MANUAL DE MENTENANȚĂ

Furnizorul va pune la dispoziția Beneficiarului manuale ce conțin particularitățile legate de parametrii de funcționare, uneltele si sculele de demontare și testare, metodele de asamblare / dezasamblare, tehnicile de reparație, precum și alte informații necesare pentru realizarea unui program de reparații și mentenanță.

Manualele vor include, de asemenea, procedurile de revizie, precum si programul (periodicitatea) acestora, indicându-se în detaliu uneltele și facilitățile necesare.

3.Cerințe de garanție si suport tehnic pentru echipamentul livrat

3.1 Toate echipamentele furnizate trebuie să fie noi si să beneficieze de o garanție de minim 24 de luni de la data livrării asigurate de producătorul acestora;
3.2 Nu se accepta produse refurbished sau remarketed;
3.3 Serviciile de garanție si suport tehnic pentru echipamente vor asigura înlocuirea oricărei componente, toate costurile înlocuirii legate de piese de schimb, manopera si orice alte cheltuieli asociate fiind suportate de către furnizorul produselor;
3.3 Timpul de reparație: Maxim 5 de zile de la sesizarea adresata de către Achizitor.

Șef Serviciul Comunicații și IT
(cu atribuții delegate)
Iustin OBREJA