41512/08,11,2022

CAIET DE SARCINI

Extindere locații Telecom+Cyber pentru sistemul SCADA și sistemul cântare

SPECIFICAȚII TEHNICE

CUPRINS

1. Generalități

1.1 Date Generale

1.1.1 Prezentul Caiet de Sarcini contine principalele cerinte minimale ce trebuie indeplinite de catre Ofertant in vederea contractarii serviciilor de proiectare, furnizare, configurare si instalare de noi locatii de telecomunicatii, inclusiv a solutiei de securitate a serviciilor Ethernet, in cadrul Sistemului de Telecomunicatii al Beneficiarului. Transmiterea datelor din aceste locatii se va efectua prin conexiuni externe VPN, puse la dispozitie de Beneficiar.

1.1.2 Execuția lucrărilor trebuie să fie realizată în conformitate cu prevederile standardelor de calitate și a legislației în vigoare.

1.1.3 Prezentele specificații nu înlocuiesc celelalte acte normative legislative și de execuție care vor trebui să fie cunoscute și respectate pe parcursul desfășurării lucrărilor.

1.1.4 Înaintea întocmirii ofertei, Ofertantul va vizita amplasamentul lucrărilor și va prezenta în acest sens un document semnat pe propria răspundere care să confirme faptul că și-a însușit condițiile din teren privind execuția lucrărilor. Lucrările trebuie să se execute în ordinea descrisă în desfășurător (etapizarea lucrărilor).

1.1.5 Oferta trebuie să fie prezentată atât pe hârtie cât și în format electronic « searchable ».

2. Prezentarea ofertei

2.1 Toate cerințele prezentului Caiet de Sarcini trebuie să fie îndeplinite de către ofertanți. Ofertele care nu respectă aceste cerințe vor fi excluse din licitație.

2.2 Răspunsurile trebuie să confirme îndeplinirea cerințelor din fiecare poziție și paragraf din Caietul de Sarcini și fiecare afirmație de conformitate trebuie susținută de ofertant cu trimiteri clare la specificațiile de firmă care certifică conformitatea declarată îndicând explicit documentul, manualul, pagina, articolul, paragraful, figura, certificatul, etc. Vor fi incluse copii de documente relevante în fiecare caz.

2.3 Oferta va contine obligatoriu preturile detaliate pentru fiecare modul hardware/software/licenta/server/etc din fiecare locatie.

2.4 Oferta trebuie să fie structurată pe formatul și numerotarea prezentului Caiet de Sarcini.

2.5 Oferta trebuie să fie prezentată în limba română. Documentația tehnică ce insoțește oferta trebuie să fie prezentată în limba română sau engleză.

3. Scopul Serviciilor

3.1 Acest Caiet de Sarcini se refera la proiectarea, furnizarea, configurarea și instalarea unei soluții de securitate a serviciilor Ethernet, si va avea în componența sa toate modulele/echipamentele/licențele (permanente neexpirabile)/etc, necesare functionarii solutiei.Locatiile ce fac obiectul proiectului sunt cele din tabelul de mai jos, la care se adauga locatia Sediu Central 2 din Ploiesti str. Rezervoarelor nr. 8 , unde vor fi instalate serverele pentru managementul solutiei:

Nr.crt	Total	Cabinet	Modul SCADA	Modul NGFW	UPS	Config	P&I&A
1	R. Moinesti	1	0	1	1	1	1
2	R. Berca	1	0	1	1	1	1
3	R. Independenta	0	1	1	0	1	1
4	Urziceni	0	1	1	0	1	1
5	R. Suplac	0	0	1	0	1	1
6	R. Marghita	0	1	1	0	1	1
7	R. Pecica	0	1	1	0	1	1
8	R. Salonta	1	0	1	1	1	1
9	R. Imeci	1	0	1	1	1	1
10	R. Ciresu	0	1	1	0	1	1

Legenda : Cabinet=cabinet de telecomunicatii de interior, 19 inchi, minim 4U, montabil pe perete sau podea.

SCADA= modul hardware/software de sniffing al datelor SCADA.

NGFW=modul hardware/software Next Generation Firewall.

Numarul maxim de active OT pentru fiecare locatie este de 5 buc. Numarul maxim de device-uri IT+OT din fiecare locatie este de 10 buc.Volumul estimat de trafic OT din fiecare locatie este de maxim 5 Mbps. Volumul estimat de trafic OT+IT din fiecare locatie este de maxim 15 Mbps.

Echipamentele SCADA+NGFW de mai sus pot fi ofertate in varianta hardware sau virtualizate software pe un device hardware. In ambele variante, hardware-ul ofertat trebuie sa respecte urmatoarele cerinte:

- temperatura de functionare -25 +60 ℃
- racire pasiva (fara ventilatoare)
- alimentare AC 220 v.
- putere consumata maxima 35 W
- certificate IEC 61850-3 si IEEE 1613

In toate locatiile vor fi configurate un numar minim de 4 VLAN-uri.Beneficiarul va putea adauga ulterior altele.

Pentru locatia Sediu Central 2 se vor livra, instala si configura server/servere de management operational si functional ale celor 2 tipuri de module de mai sus.

UPS= echipament SMT1500RMI2UC sau similar.

Config= lucrari de configurare software (inclusiv retelele de date VLAN Intranet, Leak Detection, Scada, Cântare, etc.), configurare tunele IPSec si management remote al tuturor echipamentelor din locatiile de mai sus.

P&I&A=lucrari de proiectare si instalare hardware, inclusiv alimentarea cu energie electrica de la tabloul Beneficiarului (aflat la o distanta maxima de 20 m), pentru cabinetele de telecomunicatii, As-built.

Pentru toate aplicatiile, softurile, echipamentele, etc. furnizate in acest proiect, Beneficiarul va avea acces total la conturile de administrare si configurare (admin, root, expert, etc).

3.2 Solutia de Securitate va avea o arhitectura distribuita, care va împiedica atacurile cibernetice la nivelul punctelor de acces ale infrastructurii operationale, respectiv echipamentele de retea de proces si retea de comunicatii, atat fizice cat si virtuale. Aceasta va consta in instalarea la nivel de site-uri a unor module hardware/software care sa permita implementarea diverselor functii de Securitate. Solutia de securitate va fi complet izolata de accesul la Internet si va rula in totalitate « on premise ». Conexiunea la internet este permisa doar in mod manual, pentru actualizari.

3.3 Aceste functii de securitate trebuie sa asigure detectarea comportamentului anormal al retelei operationale, descoperirea atacurilor de tip “0-Day”, atacuri evazive, atacuri bazate pe script, segregarea retelei pentru prevenirea miscarilor laterale in cazul unei intruziuni, prevenirea atacului de tip MiM (Man in the Middle), DoS, Watering hole.

3.4 Solutia trebuie sa ofere platforma centralizata pentru identificarea si managementul riscurilor de Securitate, bazata pe colectarea, validarea, corelarea si analiza informatiilor primite de la modulele distribuite, si pe care sa le prezinte intr-un mod unitar si agregat, printr-o interfata grafica (GUI). Pentru toate modulele software ce vor fi furnizate, Prestatorul va livra kit-urile de instalare și licențele aferente, permanente, neexpirabile.

3.5 Solutia de Securitate trebuie sa aiba capacitatea de a adăuga aplicații/functii de securitate atunci când este necesar.

3.6 Solutia va furniza functionalitatile de Securitate asa cum sunt specificate in sectiunile urmatoare :

A) Modul NGFW trebuie sa asigure filtrarea traficului de intrare si de iesire din locatie pe baza unui set de reguli définit de Beneficiar si trebuie sa indeplineasca urmatoarele functionalitati:

- să separe retelelele securizate de retelele nesecurizate;
- să filtreze accesul la Internet/Intranet;
- să foloseasca canalul de control securizat și criptat;
- să suporte IPSec VPN, NAT, controlul identitatii;
- să furnizeze o analiză a header-elor;
- să sigure protectie impotriva IP spoofing;
- să ofere managementul de stare în cadrul sesiunii complete (full-session state management);
- să furnizeze ACL bazat pe IP / Port / User;
- să asigure controlul aplicațiilor (application control) prin crearea de politici granulare care identifica, blocheaza sau limiteaza utilizarea unei aplicatii;
- sa valideze că o aplicație este autorizată să utilizeze un port de comunicare specific, pe baza indicatorilor găsiți în header-ul pachetului;
- să valideze utilizarea autorizata a protocoalelor SCADA suportate;
- să ofere granularitate pentru definirea politicilor de autorizare, bazate pe protocolul SCADA specific, precum și setul de comenzi autorizate din cadrul acelui protocol;
- să furnizeze IPS (Intrusion Prevention) împotriva traficului de rețea rău intenționat și nedorit. Modulul IPS trebuie actualizat în mod regulat cu noi mijloace de apărare împotriva amenințărilor emergente. Trebuie să fie posibilă actualizarea IPS online.
- să inspecteze, să scaneze și să securizeze traficul criptat SSL care trece prin gateway.
- să fie posibilă actualizarea tuturor platformelor distribuite offline dintr-o locație centralizată.
- sa fie furnizate log-uri pentrua analiza istoricului de evenimente
- sa fie capabila să înregistreze evenimentele capturate de pe toate echipamentele retelei operationale identificate, pentru o perioadă de 6 luni

- sa aiba configuratia serverului/serverelor care sa permita procesarea tuturor evenimentelor și datele de activitate pentru o perioadă de 6 luni
- sa aiba capacitatea de a stoca centralizat logurile și configuratiile tuturor echipamentelor retelei operationale pentru o perioadă de 6 luni.

Toate modulele NGFW instalate in locatii vor fi gestionate functional si operational de la o singură platforma centralizată de management. În cazul în care este necesar hardware sau software suplimentar, ofertantul trebuie să îl includă în oferta tehnica si comerciala.
Ofertantul trebuie sa ofere o descriere a solutiei.

B) Functia de Criptare trebuie sa asigure securizarea arhitecturii de comunicatii intre site-uri si serverul central.
Nivelul de criptare trebuie să fie cel puțin la fel de puternic ca nivelul de criptare furnizat de TLS 1.2, AES256-SHA256.
Canalul de comandă trebuie sa fie securizat și criptat.
In ceea ce priveste topologia, Solutia trebuie sa poata cripta orice serviciu in topologie P2P, P2MP, MP2MP.
Ofertantul trebuie sa ofere o descriere a solutiei.
Activarea functiilor **A)** si **B)** pe un port nu trebuie sa duca la scaderea semnificativa a vitezei de transfer a datelor (throughput minim 50%)

C) Modul SCADA trebuie sa colecteze datele prin « port mirroring » pentru a detecta comportamentul si activitatile anormale pentru reteaua operationala SCADA.
Aceasta functie trebuie sa analizeze traficul si sa genereze alerte in situatiile in care au fost identificate operatiuni anormale asupra retelei SCADA. Alertele trebuie sa fie trimise in timp real catre platforma centralizata de management si evaluare a riscurilor.
Pentru fiecare element al retelei operationale, trebuie sa furnizeze cel putin urmatoarele informatii :

- adresa IP v4
- producatorul
- tipul si modelul echipamentului
- adresa MAC
- data primei si ultimei aparitii in retea
- rolul elementului
- traficul de date efectuat
- locatia in cadrul retelei
- protocoalele utilizate
- gradul de vulnerabilitate
- interfata grafica in care sa fie reprezentate toate device-urile retelei, topologia si sesiunile de date active dintre ele.
- inventar al numarului device-urilor reale din retea.
- fisiere PCAP pentru analize ulterioare ale evenimentelor.
- valori ale traficului din retea, protocoalelor utilizate si sesiunilor active, atat in timp real cat si anterior.
- transmiterea configurabila a alertelor, incidentelor, etc catre adrese de email stabilite.
- compatibilitate completa cu echipamentele OT ABB -RTU560 protocol IEC104.
- detectare comportament necorespunzator al protocoalelor SCADA.
- inspectare pachetele de date (DPI – Deep Packet Inspection) pentru a arata protocolul de date utilizat si a realiza un profil de trafic SCADA in mod automat; perioada pentru "invatarea" profilului de trafic trebuie sa fie de maxim 30 de zile, cu posibilitatea reinitializarii perioadei de invatare in orice moment in functie de modificarea retelei SCADA si a deciziei Beneficiarului.

Soluția trebuie sa includa cel putin urmatoarele functionalitati :

- să ruleze pe baza unor reguli care alocă potrivirea profilului de pachete cu semnăturile (IDS) si să poată efectua analiza acestora. Ofertantul trebuie să descrie procesul de analiză.
- sa fie complet automata, sa nu necesite configurarea unor reguli asemănătoare firewall-ului, nici definirea protocoalelor de monitorizare și a alertelor pe care să le genereze.
- să specifice direcția canalelor de comunicații (sursă și destinație). Canalul de comanda trebuie securizat si criptat.
- să prezinte statistici ale pachetelor trimise și recepționate de către dispozitive in reteaua operationala.
- să genereze automat o hartă a tuturor dispozitivelor monitorizate.
- sa suporte protocoalele SCADA minim IEC-104 si Modbus.
- sa identifice asset-urile OT fizice reale din retea si localizarea acestora.
- sa utilizeze regulile Yara, CVE, MITRE ATT&CK.
- sa contina baza de date cu dispozitivele detectate in reteaua operationala, cu atributele acestora, astfel încât acestea să fie recunoscute automat în timpul analizei. Dispozitivele detectate sa fie atat echipamentele SCADA cat si echipamentele de comunicatii nivel 2 si nivel 3 conectate la reteaua operationala.
- sa permita un mecanism de căutare dupa atributele dispozitivelor, cum ar fi numele dispozitivului, adresa MAC, numele de utilizator al rețelei, adresa IP, tag-uri, adresele IP externe, comenzi SCADA.
- să poată defini propriile descrieri (marcare) pentru dispozitivele din rețea pentru o căutare și identificare mai bună.
- să permită căutarea de tip text a obiectelor din rețea și ulterior sa afiseze activitatea respectivelor dispozitive in istoricul listelor de activitati.
- sa includa generarea de rapoarte configurabile, la cerere sau programate, in format pdf si csv, prin email sau download.
- sa includa posibilitatea de a modificare configuratie sau analiza activitate din linia de comanda CLI.
- sa defineasca intarzierile introduse de functionalitatile activate pe fiecare canal in parte.

- sa se integreze nativ tehnologic cu Firewall-ul de la punctul A).
- sa utilizeze un server NTP configurabil.
- sa identifice cel putin urmatoarele tipuri de device-uri : switch, router, printer, computer, PLC, HMI, controller, firewall, RTU, server, gateway, OT, IoT, sensor, IED.
- să colecteze informații, să analizeze activitatea comportamentală și activitatea rețelei și să aibă capabilitatea să le folosească pentru a investiga riscurile de securitate pe următoarele valori din rețea:

• Conexiuni de rețea
• Validarea protocoalelor folosite
• Dispozitive de rețea conectate
• Conexiuni active
• Detectarea mișcării caracteristice pentru malware
• Detectarea sistemului de operare
• Evenimente neobișnuite legate de activitatea dispozitivelor
• Broadcasts
• Pierderea excesivă a conexiunilor
• Interogări DNS catre servere externe
• Factor de transfer extern de date (rata de descărcare pentru datele descărcate)
• Factor de transfer intern de date (rata descărcare / descărcate)
• Pachete externe trimise și primite de dispozitiv
• Fast Travel Warning - conectari rapide din diferite locații pentru același utilizator
• Atacuri asupra server FTP
• Atacuri de tip Heartbleed
• Formate de fișier invalide
• Nume invalide de host-uri
• Utilizarea de noi aplicații / protocoale pe dispozitiv
• Dispozitive noi
• Repornirea dispozitivelor
• Servere conectate la porturi non-standard
• Încărcarea excesivă a sistemelor

Toate modulele SCADA instalate in locatii vor fi gestionate operational si functional de la o singură platforma centralizată de management. În cazul în care este necesar hardware sau software suplimentar, ofertantul trebuie să îl includă în oferta tehnica si comerciala.

3.12 Functionalitatile A), B) si C) enumerate mai sus trebuie sa fie implementate cu ajutorul a maxim 2 module hardware/software in fiecare site; Toate licentele necesare vor avea caracter permanent, fara a fi necesara innoirea periodica a acestora.

3.18 Managementul centralizat al modulelor hardware/software instalate in locatii va include cel putin :
- controlul si configurarea echipamentelor distribuite;
- activarea si configurarea functiilor de Securitate pe fiecare echipament distribuit ;
- configurarea secventei functiilor de Securitate (service chaining);
- operarea si mentenanta echipamentelor distribuite.
- transmiterea de alerte si notificari de securitate prin email.

Ofertantul va descrie modul in care sunt implementate cerintele de mai sus.
3.19 Managementul centralizat va permite conectarea simultana a mai multor utilizatori, cel putin 5, printr-o conexiune securizata HTTPS/SSL. Autentificarea utilizatorilor trebuie sa se faca pe baza de nume utilizator si parola.
3.21 Soluția va fi configurată pentru a efectua backup-uri în mod automat, cel puțin odata pe zi, fără a fi nevoie de intervenția umană.
3.22 Pentru accesul remote la Managementul centralizat Prestatorul va furniza o aplicație licențiată pentru acces remote. Aceasta va permite operarea solutiei remote în mod securizat de pe laptop (sau local prin conectarea laptop-ului in acelasi LAN) și va include toate modulele/echipamentele/software-urile necesare in acest sens. Pentru acces securizat din internet la noul server, Prestatorul va furniza și configura un router/firewall . Beneficiarul va asigura conectivitatea la Internet a acestuia.

3.23 Prestatorul trebuie să furnizeze toate bunurile și serviciile descrise aici ca un proiect “la cheie” și trebuie să își asume responsabilitatea completă pentru proiectarea, livrarea, instalarea, testarea, configurarea și acceptanța echipamentelor și aplicațiilor asociate așa cum sunt specificate în acest Caiet de Sarcini.

3.24 Prestatorul trebuie să furnizeze toate materialele, echipamentele, sculele, ingineria, calificarea şi forţa de muncă necesare pentru a îndeplini în totalitate și în timp util cerinţele din acest Caiet de Sarcini.

4. Livrări

4.1 Toate echipamentele furnizate, inclusiv materialele pentru instalaţii trebuie să fie noi, neutilizate, de cea mai înaltă calitate, nedeteriorate, de fabricaţie recentă, sau de un tip fabricat în prezent. Pentru toate acestea Prestatorul va prezenta documente ale producatorilor din care sa reiasa ca echipamentele hardware/software livrate nu sunt declarate « End of Life » la data depunerii ofertei.

4.2 Orice element/modul/licență/funcționalitate/accesoriu (de exemplu: aplicatie, surse de energie, cablu alimentare, etc.) care lipsește din ofertă și care se va dovedi necesar pentru îndeplinirea cerințelor prezentului Caiet de Sarcini, trebuie să fie inclus ulterior fără nici un cost suplimentar pentru Beneficiar.

5. Servicii

5.1 Servicii de design trafic și management

Prestatorul trebuie sa furnizeze documentatii de proiectare de detaliu ale solutiei, diagrame bloc ale solutiei pe fiecare site, connectivitatea intre site-urile sursa si cele destinatie. Informatia trebuie furnizata in format electronic editabil.

Prestatorul trebuie să furnizeze manualele complete, detaliate, incluzând proceduri “step by step” de instalare, operare, configurare, programare, administrare și troubleshooting pentru echipamentele/software-urile livrate. Manualele vor fi livrate in format electronic.

5.2 Servicii de instalare

Toate lucrările de instalare (Hardware & Software) trebuie să fie efectuate în conformitate cu legile românesti, standardele naţionale şi internaţionale şi cu specificaţiile de producător. Instalarile trebuie sa fie efectuate de personal certificat de Producatorul Solutiei.

Instalarea trebuie să fie în conformitate cu cele mai bune practici industriale actuale.

Prestatorul este responsabil pentru depozitarea tuturor materialelor achiziționate de către Beneficiar până la semnarea procesului verbal de recepție.

Prestatorul trebuie să colecteze de la depozitul său şi trebuie să transporte pe site echipamentul necesar şi materialele pentru instalatii.

La finalizarea lucrărilor, întreaga zonă de lucru trebuie să fie lăsată curată şi liberă de gunoi, praf, resturi şi materiale în exces.Toate materialele utilizabile rămase în urma instalărilor vor fi predate Beneficiarului.

Prestatorul trebuie să documenteze instalarea cu imagini.

5.3 Teste de acceptanţă operaţională

5.3.1 Prestatorul va include in oferta procedura de verificare pentru acceptanță, care va include teste pentru toate functionalitatile solicitate prin Caietul de Sarcini. Procedura va fi validata de Beneficiar cu 30 de zile înainte de efectuarea testelor de acceptanță operațională.

5.3.2 Acceptanța trebuie să asigure că Solutia livrata:
• Este instalata corect conform documentatie producator;
• Este configurata corect conform documentatie producator, informatiilor de design si necesitatii Beneficiarului;
• Toate functionalitatile cerute prin prezentul Caiet de Sarcini sunt personalizate pentru prezentul proiect.
• Operează fara erori;
• Are înregistrate toate datele relevante ale commissioning-ului pentru utilizări viitoare ca referință;

5.4 Managementul Proiectului

5.4.1 Prestatorul va fi responsabil de planificarea, urmărirea și coordonarea proiectului incluzând, dacă este cazul, și planificarea și urmărirea lucrărilor subprestatorilor. Prestatorul va solicita aprobarea Beneficiarului pentru înlocuirea oricărui subprestator.

5.4.2 Prestatorul va trebui sa prezinte in echipa dedicata pentru acest proiect personal propriu certificat de producator pentru derularea activitatilor de instalare, planificare, implementare, administrare si mentenanta a echipamentelor hardware si software livrate.

5.4.3 Prestatorul trebuie să desemneze un Project Manager al cărui CV trebuie să fie anexat documentaţiei de calificare şi care trebuie să evidenţieze studiile relevante şi experienţa persoanei desemnate de ofertant în managementul unor proiecte

similare ca obiect şi amploare. Componența echipei prezentată în ofertă va putea fi schimbată numai cu aprobarea Beneficiarului.

5.4.4 Minute ale întalnirilor Prestator-Beneficiar trebuie să fie întocmite de către Prestator şi vor fi disponibile ca bază pentru deciziile luate la reuniunile periodice de progres.

6. Receptia la terminarea lucrarilor

6.1 Termenul de finalizare a serviciilor din Caietul de Sarcini se consideră împlinit la data semnării fără obiecțiuni de către Comisia de recepție a Procesului verbal de recepție, după terminarea ultimului test de acceptanță operațională.

6.2 Prestatorul are obligația de a livra cu 30 de zile inainte de finalizarea lucrarilor documentatia tehnica a Solutiei, respectiv „As built". Prestatorul va comunica Beneficiarului data finalizării lucrarilor transmițându-i acestuia, pentru confirmare, o înștiințare scrisă. Documentatia „As built" va include proceduri scrise detaliate ale operațiilor necesar a fi efectuate de Beneficiar pentru utilizarea cu succes a soluției, luând în considerare toate situațiile posibile ce pot apare în operarea soluției. Documentatia "As built" va contine deasemenea arhitectura detaliata a tuturor componentelor solutiei livrate si a conexiunilor interne. Prestatorul va furniza deasemenea manualul conținând toate comenzile CLI necesare în configurarea, operarea și mentenanța soluției.

6.3. Beneficiarul va organiza recepția în maximum 5 zile de la notificarea finalizării serviciilor și va comunica Prestatorului data stabilită.

6.4 Comisia de recepție trebuie să verifice execuția tuturor lucrărilor conform prevederilor contractuale și documentației anexate la contract, după care întocmeste "Procesul verbal de recepție" și recomandă admiterea cu sau fără obiecțiuni a recepției, amânarea sau respingerea ei, conform modului de îndeplinire a condițiilor contractuale.

7. Garanţie

7.1 Prestatorul trebuie să furnizeze Beneficiarului garanție comerciala de 1 an de la data semnării procesului verbal de recepție pentru toate echipamentele furnizate, modulele hard/soft, licențele și lucrările efectuate .

7.2 Acestă garanție trebuie să includă repararea sau înlocuirea oricărui echipament, subsistem, hardware și/sau software care s-a defectat în condiții normale de uzură și de utilizare. Această activitate va include montarea/demontarea și transportul aferent.

7.3 In perioada de garantie Beneficiarul va avea la dispozitie posibilitatea de deschidere de tichete de asistenta direct la producatori, cu timp de raspuns de maxim 30 minute, pentru rezolvarea eventualelor probleme aparute. Prestatorul va deschide conturi pe numele Beneficiarului la producatorii solutiilor furnizate si va acorda acestuia acces total la aceste conturi.

7.4 Prestatorul trebuie să organizeze şi să furnizeze intervenţie pe site/remote în maxim 8 ore (business hours) atunci când este semnalată de către Beneficiar nefuncționarea sau funcționarea defectuoasă a echipamentelor

7.5 Prestatorul trebuie să presteze servicii Swap de reparare prin schimbare pe site, cu un timp de swap de maxim 2 zile.

7.6 Prestatorul trebuie să anexeze la oferta tehnică documentul „Propunere pentru asigurarea intervenţiei în amplasamente, în perioada de garanţie", în care trebuie să descrie în detaliu modalităţile prin care va asigura îndeplinirea timpilor de remediere asumaţi.

7.7 Acolo unde o functionare defectuoasă a fost corectată, înlăturată sau înlocuită în garanție, perioada de garanție corespunzătoare acestei lucrări va fi extinsă cu perioada de nefuncționare după ce această corecție de înlăturare și înlocuire a fost îndeplinită cu succes.

7.8 Pe perioada garantiei Prestatorul trebuie să furnizeze gratuit atat upgrade-uri cat si update-uri/patch-uri pentru toate software-urile livrate, inclusiv pentru semnaturile malware (Firewall, VPN, Application Control, URL Filtering, IPS/IDS, Antibot, Antivirus, etc) si managementul centralizat.

8. Etapizarea lucrărilor

8.1 Proiectare integrala detaliata a solutiei- 1 luni de la semnarea contractului.

8.2 Livrare echipamente/software – maxim 3 luni de la semnarea contractului.

8.3 Instalare echipamente si integrare software – maxim 2 luni de la livrarea echipamentelor.

8.4 Teste acceptanță operațională și predare documentație As built – 1 luni de la terminarea lucrărilor de instalare. In cazul respingerii unora dintre testele de acceptanta, problemele semnalate trebuie remediate in termen de maxim 5 zile. Dupa aceasta testele de acceptanta vor fi reluate in integralitatea lor. Procedura se repeta pana la finalizarea cu succes a tuturor testelor. Beneficiarul nu accepta prelungirea termenului de executie a contractului datorita eventualelor repetari ale testelor de acceptanta.

8.5 La solicitarea Prestatorului, Beneficiarul poate aproba decalarea termenelor etapelor intermediare, fără a se modifica termenul final al Contractului.

8.6. Termenul de execuție a tuturor serviciilor contractate este de 6 luni de la semnarea contractului.

Sef Departament Dezvoltare Mentenanta
Ing. Dan Buzatu

Dan Buzatu Digitally signed by Dan Buzatu
Date: 2022.11.08 09:40:58 +02'00'

Sef Serviciu Telecomunicatii
Ing. Catalin Ruse

Intocmit Catalin Ruse Digitally signed by Catalin Ruse
Date: 2022.10.13 12:08:08 +03'00'
Coordonator activitate
Ing. Iulian Bucur

Iulian Bucur Digitally signed by Iulian Bucur
Date: 2022.10.13 12:06:46 +03'00'