

DISTRIBUTIE ENERGIE OLTENIA SA

Aprobat de:
Eugen Butoarca
COO - Membru Directorat

Vizat de:
Miron Alba
Director Directie - Divizia strategie si dezvoltare active

CAIET DE SARCINI

**Asigurarea securitatii cibernetice a sistemelor informatice utilizate in
DEO - Achizitie solutie securitate si virtualizare pentru sistemul SCADA**

Avizat de:
Sandulescu Cristian
Director Directie ICT

Avizat de:
Magdalena Silvia ROTARU SIMION
Manager Departament SSM

Pregatit de:
Radu Sanda
Manager Departament ICTO

Cuprins

1.	Lista abrevierilor si terminologiei folosite	4
1.1	Prescurtari / abrevieri	4
1.2	Definitii	4
2.	Partea contractantă.....	5
3.	Obiectul procedurii de achizitie	5
3.1	Descrierea obiectului contractului	5
4.	Introducere.....	6
4.1	Contextul Realizarii Acestei Achizitii De Produse	6
4.1.1	Informatii Despre Autoritatea/Entitatea Contractanta	6
4.1.2	Informatii Despre Contextul Care A Determinat Achizitionarea Produselor	7
4.1.3	Informatii Despre Beneficiile Anticipate De Catre Autoritatea/ Entitatea Contractanta	7
4.1.4	Cadrul General Al Sectorului În Care Autoritatea/Entitatea Contractanta Îsi Desfasoara Activitatea	7
4.2	Descrierea Situatiei Actuale La Nivelul Entitatii Contractante.....	8
4.3	Obiectivul General La Care Contribuie Furnizarea Produselor	8
4.3.1	Obiectivul Specific La Care Contribuie Furnizarea Produselor.....	9
4.4	Durata contractului de furnizare produse.....	9
5.	Specificatii tehnice.....	9
5.1	Dezvoltare solutie securitate de protectie aplicatii web si api.....	9
5.2	Dezvoltare sistem de comunicatii securizate de backup pentru dispecerate	12
5.3	Dezvoltare sistem management incidente.....	17
5.4	Dezvoltare Solutie Load Balancer	33
5.5	Dezvoltare Solutie securitate ICS	35
5.6	Dezvoltare solutie de autentificare si autorizare protaluri web	42
5.7	Dezvoltare platforma de virtualizare securizata	44
5.8	Echipamente 802.1x SCADA	45
5.9	Servicii Configurare	47
6.	Punere în functiune, testare.....	51
7.	Garantie.....	51
8.	Livrare, ambalare, etichetare, transport si asigurare pe durata transportului	53
8.1	DOCUMENTATII CE TREBUIE FURNIZATE ENTITATII CONTRACTANTE ÎN LEGATURA CU PRODUSUL	54

CAIET DE SARCINI

8.2	RECEPTIA PRODUSELOR.....	54
8.3	MANAGEMENTUL/GESTIONAREA CONTRACTULUI SI ACTIVITATI DE RAPORTARE ÎN CADRUL CONTRACTULUI.....	55
9.	Cerințe privind Practicile Etice, Conduita în Afaceri și Conformitatea:	56
10.	Cerințe privind prelucrarea DCP	57
11.	Cerințe SSM, aplicabile in perioada de derulare a contractului.....	57
11.1	Cerinte SSM privind obligatiile contractantilor	57
11.2	Conditii privind sanatatea si securitatea muncii la executarea lucrarilor/ prestarea serviciilor ...	58
12.	ANEXE	61
13.	Reglementari aplicabile care trebuie respectate	61

1. Lista abrevierilor si terminologiei folosite

1.1 Prescurtari / abrevieri

„**DCP**” – Date cu caracter personal, însemnând orice informație referitoare la o persoană fizică identificată sau identificabilă să fie identificate, direct sau indirect, în special prin referire la un identificator cum ar fi un nume, un număr de identificare, date despre locație, un identificator online sau unul sau mai mulți factori specifici de ordin fizic, fiziologic, genetic, mental, economic, cultural sau privind identitatea socială a acelei persoane fizice.

„**GDPR**” - Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea DCP și libera circulație a acestor date (Regulamentul general privind protecția datelor).

1.2 Definitii

„**Zile**” - se va intelege zile calendaristice, daca nu va fi mentionat altfel

„**DEO**” - DISTRIBUTIE ENERGIE OLTENIA S.A

„**Caiet de Sarcini**” – set de documente privind achiziția de produse inclusiv anexele la acestea sau la care se face referire în acestea.

„**GDPR**” sau „**Regulamentul privind protectia datelor cu caracter personal**” - Regulamentul (UE) nr. 679/27.04.2016 al Parlamentului European si al Consiliului privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE.

„**Notificarea de confidentialitate**” – comunicare în forma scrisă adresată sau pusă la dispoziția persoanelor vizate de activități de prelucrare a datelor cu caracter personal, prin care acele persoane sunt informate cu privire la activitățile de prelucrare a datelor acestora, scopul prelucrărilor, categoriile de date cu caracter personal implicate, temeiurile juridice ale prelucrărilor, obligațiile operatorului de date cu caracter personal și ale imputernicitorilor acestuia, drepturile persoanelor vizate cu privire la datele afectate de respectivele prelucrări, modalități de a comunica cu operatorul, precum și alte informații relevante cu privire la respectivele prelucrări de date.

„**Chestionarul de conformitate GDPR**” – set de întrebări (prezentat în Anexa la Caietul de Sarcini) vizând maniera în care un ofertant respectă regulile și obligațiile ce îi revin cu privire la protecția DCP.

„**Prelucrarea DCP**” – are semnificația prevăzută în GDPR, adică „orice operațiune sau set de operațiuni care se efectuează asupra datelor cu caracter personal sau pe seturi de date cu caracter personal, indiferent dacă sunt sau nu prin mijloace automatizate, cum ar fi colectarea, înregistrarea, organizarea, structurarea, stocarea, adaptarea sau modificarea, recuperarea, consultarea, utilizarea, dezvoltarea prin transmitere, diseminarea sau punerea la dispoziție în alt mod, alinierea sau combinarea, restricționarea, ștergerea sau distrugerea”.

“**Capitolul privind prelucrarea DCP**” – un capitol ce se va introduce imediat anterior capitolului “Prevederi finale” din contractul de achiziție care se va încheia cu ofertantul câștigător, prevăzând drepturile și obligațiile părților la contract în legătură cu orice activități de prelucrare a datelor cu caracter personal care apar în executarea acelui contract.

2. Partea contractantă

DISTRIBUTIE ENERGIE OLTENIA S.A., str. Calea Severinului nr.97, RO 14491102

3. Obiectul procedurii de achiziție

Încheierea unui contract pentru o 'Soluție securitate și virtualizare pentru sistemul SCADA' din centrele de date ale *Distribuție Energie Oltenia SA* cât și achiziția unei soluții de coordonare, planificare și răspuns automat la amenințările de securitate adresate sistemelor informatice *Distribuție Energie Oltenia SA*

Prezentul caiet de sarcini cuprinde specificațiile tehnice pentru achiziția produselor descrise mai jos.

3.1 Descrierea obiectului contractului

Se vor achiziționa, instala, configura și integra în rețeaua Distribuție Energie Oltenia SA următoarele:

Nr crt	Denumire produs	UM	Cantități contract
1	Dezvoltare soluție securitate de protecție aplicații web și API	Buc.	1
2	Dezvoltare sistem de comunicații securizate de backup pentru dispecerate	Buc.	1
3	Dezvoltare sistem management incidente	Buc.	1
4	Dezvoltare Soluție Load Balancer	Buc.	1
5	Dezvoltare Soluție securitate ICS	Buc.	1
6	Dezvoltare soluție de autentificare și autorizare portaluri web	Buc.	1
7	Dezvoltare platforma de virtualizare securizată	Buc.	1
8	Echipamente 802.1x SCADA	Buc.	1

Livrarea și instalarea produselor se va efectua la locația Distribuție Energie Oltenia Craiova aflată la adresa de mai jos:

Distribuție Oltenia – Craiova – jud. Dolj – str. Nicolae Titulescu nr.1

Furnizorul se obliga sa livreze, instaleze, configureze si sa integreze produsele in maxim 90 de zile de la semnarea contractului de ambele parti

4. Introducere

Caietul de sarcini face parte integranta din documentatia de atribuire si constituie ansamblul cerintelor pe baza carora se elaboreaza de catre fiecare ofertant propunerea tehnica.

Caietul de sarcini contine, specificatii tehnice. Acestea definesc, dupa caz si fara a se limita la cele ce urmeaza, caracteristici referitoare la nivelul calitativ, tehnic si de performanta, siguranta în exploatare, dimensiuni, precum si sisteme de asigurare a calitatii, terminologie, simboluri, teste si metode de testare, ambalare, etichetare, marcare, conditiile pentru certificarea conformitatii cu standarde relevante sau altele asemenea.

În cadrul acestei proceduri, Distribuție Energie Oltenia îndeplinește rolul de Entitate Contractanta, respectiv Entitatea Contractanta în cadrul Contractului.

Pentru scopul prezentei secțiuni a Documentatiei de Atribuire, orice activitate descrisa într-un anumit capitol din Caietul de Sarcini si nespecificata explicit în alt capitol, trebuie interpretata ca fiind mentionata în toate capitolele unde se considera de catre Ofertant ca aceasta trebuia mentionata pentru asigurarea îndeplinirii obiectului Contractului.

4.1 Contextul Realizarii Acestei Achizitii De Produse

4.1.1 Informatii Despre Autoritatea/Entitatea Contractanta

Distribuție Energie Oltenia SA, persoana juridica româna, cu capital privat, care este organizata si functioneaza în conformitate cu dispozitiile legale în vigoare si cu statutul propriu, având ca obiect principal activitatea de distributie a energiei electrice si servicii adiacente, în conditiile prevazute de statutul societatii si în licenta de operare nr. 457 / 15.03.2007, pentru distributie a energiei electrice, acordata de Autoritatea de Reglementare în domeniul Energiei (ANRE). Potrivit art. 44 si art. 441 din Legea nr. 123/2012 a energiei electrice si a gazelor naturale, distributia energiei electrice se realizeaza de catre operatorul de distributie, persoana juridica, titulara de licenta, activitatea de distributie a energiei electrice, cu exceptia celei realizate prin sistemele de distributie inchise, constituind serviciu public de interes general.

Distribuție Energie Oltenia SA, denumita în cele ce urmeaza si DEO, asigura serviciile de distributie a energiei electrice în judetele Arges, Dolj, Gorj, Olt, Mehedinți, Teleorman si Vâlcea, si deserveste un numar de aprox. 1,44 milioane consumatori, situati într-o arie de acoperire de aproximativ 42.134 km².

În temeiul Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelilor și sistemelor informatice, Distribuție Energie Oltenia S.A. a solicitat înscrierea în ROSE pentru sectorul ENERGIE, subsectorul ELECTRICITATE. Ca urmare, ACNNISS a emis Decizia nr. A-1010/I din 27.10.2020 privind înscrierea DISTRIBUȚIE ENERGIE OLTENIA S.A. in Registrul operatorilor de servicii esentiale (ROSE).

4.1.2 Informatii Despre Contextul Care A Determinat Achizitionarea Produselor

Standardul de performanta, aprobat prin ordin ANRE nr. 46/2021, al distributiei energiei electrice stabileste atat prevederi noi pentru DEO, precum si indicatori privind calitatea serviciului de distributie.

Standardul reglementeaza 3 categorii de indicatori de performanta:

- continuitatea alimentarii cu energie electrica a utilizatorilor;
- calitatea tehnica a energiei electrice distribuite;
- calitatea comerciala a serviciului de distributie a energiei electrice.

In vederea asigurarii unui nivel ridicat de securitate a retelelor si sistemelor informatice, DEO, in calitate de operator de servicii esentiale, va proceda la punerea in aplicare a tuturor prevederilor Legii nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a retelelor si sistemelor informatice, cu modificarile si completarile ulterioare, aplicabile operatorilor de servicii esentiale.

4.1.3 Informatii Despre Beneficiile Anticipate De Catre Autoritatea/ Entitatea Contractanta

DEO a stabilit o serie de obiective si tinte care sa conduca la indeplinirea conditiilor stabilite de catre Standardul de performanta, precum si la scaderea indicatorilor de performanta. Aceste obiective sunt:

Cresterea gradului de satisfactie a clientilor; aceasta tinta urmareste cresterea gradului de furnizare a serviciului catre clienti în conditii normale, însoțit de reducerea numarului reclamatiiilor acestora privind functionarea normala a furnizarii energiei electrice.

Entitatea Contractanta a identificat o serie de beneficii pe care le va obtine in urma automatizarii retelei de distributie si din care se remarca urmatoarele:

- a) *Cresterea disponibilitatii retelei de joasa tensiune*
- b) *Cresterea gradului de satisfactie a clientilor*

Entitatea Contractanta a identificat o serie de beneficii care vor fi oferite consumatorului final de energie electrica prin cresterea calitatii energiei electrice prin reducerea numarului de intreruperi si a duratei acestora.

De asemenea, avand in vedere Ordinul nr. 1323/2020 pentru aprobarea Normelor tehnice privind cerințele minime de asigurare a securității rețelor și sistemelor informatice aplicabile operatorilor de servicii esențiale, DEO a stabilit o serie de achizitii necesare în vederea respectarii cerintelor minime.

4.1.4 Cadrul General Al Sectorului În Care Autoritatea/Entitatea Contractanta Îsi Desfasoara Activitatea

Principalele autoritati de reglementare din sectorul energetic sunt: Autoritatea Nationala de Reglementare în Domeniul Energiei (ANRE), Autoritatea Nationala de Reglementare pentru Serviciile Comunitare de Utilitati Publice (ANRSC), Autoritatea Nationala pentru Administrare si Reglementare în Comunicatii (ANCOM), Ministerul Economiei, Ministerul pentru Mediul de Afaceri, Ministerul Energiei, si Consiliul Concurentei.

Legislatia (impune actualizarea cadrului de reglementare necesar functionarii sectorului si pietei

energiei electrice și a gazelor naturale în condiții de eficiență, concurență, transparență și protecție a consumatorilor, precum și implementării și monitorizării măsurilor de eficiență energetică.

Legea nr. 362/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice transpune în legislația națională Directiva (UE) 2016/1148 (NIS) a Parlamentului European și a Consiliului din 6 iulie 2016 privind măsuri pentru un nivel comun ridicat de securitate a rețelelor și a sistemelor informatice în Uniune.

Implementarea Legii NIS la nivelul României intră în atributul Centrului Național de Răspuns la Incidente de Securitate Cibernetică, CERT-RO, prin Autoritatea competentă la nivel național pentru securitatea rețelelor și sistemelor informatice, denumită în continuare ANSRSI.

4.2 Descrierea Situației Actuale La Nivelul Entității Contractante

Entitatea Contractantă realizează servicii de distribuție a energiei electrice în concordanță cu standardul de performanță.

În situația actuală, se dorește implementarea unui sistem de virtualizare dedicat împreună care să includă și o soluție integrată de securitate bazată pe aparate fizice. Soluția de securitate trebuie să permită crearea de politici de acces granulare atât nord-sud cât și est-vest imediat centralizat.

În aceste condiții, DEO SA a stabilit o serie de obiective și ținte care să conducă la îndeplinirea condițiilor stabilite de către Standardul de performanță, precum și la scăderea indicatorilor de performanță DEO, în calitate de operator de servicii esențiale, are obligația de a pune în aplicare toate prevederile Legii nr. 363/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice, cu modificările și completările ulterioare, aplicabile operatorilor de servicii esențiale.

4.3 Obiectivul General La Care Contribuie Furnizarea Produselor

Pornind de la obiectivele societății și în concordanță cu nivelul tehnic actual al instalațiilor, DEO a adoptat o strategie de dezvoltare a rețelelor electrice de distribuție, prin care urmărește o abordare uniformă și coerentă a conceptelor strategice, țelul final conducând la:

1. îmbunătățirea stării tehnice a instalațiilor de distribuție a energiei electrice;
2. reducerea pierderilor de energie electrică, tehnice și comerciale;
3. asigurarea creșterii capacității de distribuție pentru preluarea noilor consumatori și/sau susținerea creșterii sarcinii consumatorilor existenți;
4. eliminarea neconformităților privind electrosecuritatea RED (Rețea Electrică de Distribuție);
5. îmbunătățirea calității energiei electrice asigurate clienților;
6. reducerea costurilor de exploatare a RED.

Pornind de la obiectivele societății și în concordanță cu Legea NIS (Legea nr. 363/2018 privind asigurarea unui nivel comun ridicat de securitate a rețelelor și sistemelor informatice) DEO își propune respectarea cerințelor de asigurare a securității rețelelor și sistemelor informatice.

4.3.1 Obiectivul Specific La Care Contribuie Furnizarea Produselor

Entitatea Contractanta isi propune:

- achizitionarea produselor pentru a putea asigura realizarea lucrarilor de investitii.;
- achizitionarea produselor pentru a putea respecta cerințele minime de asigurare a securității rețelelor și sistemelor informatice aplicabile operatorilor de servicii esențiale.
- imbunatatirea conformitatii cu standardele de securitate va permite organizatiei sa respecte mai eficient reglementările internaționale, reducând astfel riscurile operaționale și financiare asociate incidentelor de securitate informatică.

4.4 Durata contractului de furnizare produse

Durata contractului: 3 luni de la semnarea contractului.

5. Specificatii tehnice**5.1 Dezvoltare solutie securitate de protectie aplicatii web si api**

Solutia tehnica ce face obiectul prezentei cereri de oferta este o combinatie de sase echipamente hardware de tip Web Application Firewall si un serviciu de protectie aplicatii web pentru cel putin 30 de site-uri/aplicatii, furnizata si gestionata conform celor mai bune practici industriale in securitatea aplicatiilor web.

Aceasta solutie trebuie sa ofere:

- Protectie completa L3-L7 pentru trafic HTTP/HTTPS
- Inspectie bidirectionala (inbound + outbound) cu protectie DLP
- Control granular al accesului si autentificarii
- Accelerare si livrare optimizata a aplicatiilor
- Inginerie de threat intelligence globala
- Extensibilitate si automatizare prin API si integrare DevOps
- Vizibilitate completa asupra traficului si a incidentelor de securitate

Toate functionalitatile urmatoare trebuie integrate nativ in solutia ofertata si inclusiv in licentierea pentru Application Protection pentru 30 de aplicatii/site-uri.

Solutia trebuie sa ofere urmatoarele functionalitati:

- Deep Inspection Bidirectionala: analiza completa a tuturor cererilor client, server si a raspunsurilor server, client pentru Data Loss Prevention (DLP), inclusiv detectarea si protectia impotriva filtrarii de date sensibile (ex: carduri, CNP, SSN).
- Website Cloaking si Server Fingerprint Suppression: abilitatea de a ascunde informatiile sensibile ale serverului (banner stripping si erori personalizate) pentru a preveni fingerprinting-ul aplicatiei de catre atacatori.
- Autentificare si Autorizare: servicii integrate pentru autentificare, autorizare si audit (AAA), inclusiv Single Sign-On (SSO), Form & Basic Authentication pre-perimetru, Integrare LDAP, RADIUS, Kerberos, SMS Passcode, RSA SecurID, SAML v2 ca Service Provider. Capacitate de a actiona drept punct central de policy pentru acces aplicatii fara a modifica aplicatiile existente.
- Management API Avansat (REST / OpenAPI): automatizare completa a politicilor, configurarilor si monitorizarii prin API REST conform specificatiilor OpenAPI, inclusiv suport pentru integrari DevOps cu Terraform, Ansible, Azure ARM, AWS CloudFormation si altele.

CAIET DE SARCINI

- Traffic Management si Accelerare Integrata: capabilitati integrate de livrare a aplicatiilor: load balancing L4/L7, caching pentru continut static/dinamic, SSL/TLS offloading. Connection pooling pentru reducerea incarcarii serverelor backend: Tunelare si rutare traficului pe baza caracteristicilor cererilor (ex: trafic desktop vs mobil).
- Threat Intelligence Global si Actualizari Automate: solutia trebuie sa beneficieze de serviciul global de Threat Intelligence, incluzand: semnături actualizate automat, feed global de telemetrie din retea distribuita, corelare a campaniilor de atac detectate la nivel mondial. Actualizari automate fara impact asupra performantei.
- Protectie Dedicata API si JSON/SOAP/GraphQL: capabilitati avansate pentru API Security, inclusiv descoperire automata, scanare si protectie impotriva atacurilor specifice API.
- Configurari Pre-Definite si Template-uri: solutia trebuie sa includa template-uri pre-configurate pentru cele mai uzuale aplicatii web (ex: WordPress, ecommerce, portaluri) care accelereaza implementarea si reduc timpul de tuning manual.
- Portal Centralizat de Management: permite administra politicilor si configuratiilor de securitate dintr-un singur loc pentru multiple instante/appliances.
- Sistem Integrat de Logare si Rapoarte Detaliat: log-uri detaliate a evenimentelor de securitate, inclusiv: System Logs, Web Firewall Logs, Access Logs, Audit Logs
- Posibilitatea exportului catre SIEM, precum Splunk si integrarea in Splunk existent.

Solutia trebuie sa ofere urmatoarele functionalitati:

- Website cloaking si protectie fingerprinting
- DLP outbound inspectand raspunsurile server
- AAA granular integrat fara modificare aplicatii
- REST API complet conform OpenAPI
- Integrari DevOps pentru orchestrare si automation
- Actualizari automate de semnături si feeds globale
- Portal centralizat pentru administrare si raportare
- Suport integrat pentru vulnerability scanner si remediation

Performanta minima obligatorie:

- Throughput criptat minim 5 Gbps.
- Minimum 50.000 tranzactii HTTPS/secunda.
- Minimum 1.800.000 conexiuni concurente.
- Suport pentru 300 servere backend per nod.
- Inspectie TLS completa cu offloading.

Specificatii hardware obligatorii:

- Format 1RU.
- Memorie ECC.
- Surse alimentare redundante hot-swap.
- Advanced Routing
- Multi-Port Hardware
- Link Bonding
- Port management dedicat.
- Interfete:
 - o minimum 8x1G Ethernet
 - o minimum 2x10G Ethernet
- NIC-uri cu bypass hardware.
- Suport VLAN, bonding, routing avansat.

Disponibilitate:

- Clustering nativ.
- Active-active si active-passive.
- Failover automat.

CAIET DE SARCINI

- Sincronizare configuratii intre noduri.
- Licentiere si scalabilitate solutie de protectie aplicatii:
- Protectie pentru minimum 30 site-uri/aplicatii distincte.
 - Implementare SaaS multi-PoP global.
 - Protectie simultana North-South si East-West.
 - Containerized WAF pentru microservicii interne.

Protectie Aplicatii si API:

Solutia combinata trebuie sa ofere:

- Protectie OWASP Top 10 Web si API.
- Smart Signatures adaptative.
- Detectie zero-day bazata pe ML.
- IP reputation + GeoIP + TOR.
- DLP outbound pentru date sensibile.
- Upload scanning antivirus + ATP.
- Cloaking aplicatie.
- Rate limiting si tarpits nelimitate.
- Descoperire automata API JSON + GraphQL.
- Shadow API discovery prin ML.
- Schema validation API.

DDoS Full-Spectrum:

- Protectie volumetrica nelimitata L3/L4.
- Protectie aplicationala L7.
- Detectie automata flood HTTP/HTTPS.
- Activare upstream scrubbing.
- Politici adaptive.

Advanced Bot Protection:

- Detectie bot ML cloud-backed.
- Credential stuffing si spraying.
- Privileged Account Protection.
- CAPTCHA + reCAPTCHA + hCAPTCHA.
- Fingerprinting client.
- Protectie brute force.
- Spam detection.

Threat Intelligence Global

- Feed global de threat intelligence.
- Telemetrie din honeypots.
- Actualizari orare.
- Corelare campanii globale.
- Semnături dinamice.

Secure Application Delivery

- TLS offload.
- Load balancing.
- CDN.
- DNS security.
- URL rewrite.
- Caching si compresie.
- HTTP/2, WebSocket, IPv6.
- Dynamic URL encryption.
- Network HSM integration.

Virtual Patching si Auto-Configuration:

- Auto Configuration Engine ML.

CAIET DE SARCINI

- Virtual patching din scanere.
- Feedback loop SOC.
- Aplicare reguli fara modificare cod.
- Sugestii automate tuning.
- Logging, SIEM si Automatizare:
 - Log complet request-level.
 - Export syslog + AMQP.
 - Conectori SIEM multipli.
 - API REST configurare.
 - JSON-based automation.
 - GitHub integration.
 - Snapshot configuratii.
 - Retentie loguri minimum 60 zile
- Servicii Hardware si Suport
 - Inlocuire hardware next-business-day pentru 3 ani.
 - Refresh hardware la 4 ani.
 - Migrare configuratie.
 - RMA global.
 - Suport 24x7.
 - Patch-uri critice.
 - Firmware continuu.
 - Early release program.
 - Update semnaturi automat.

Ambele componente ale solutiei trebuie sa fie de la acelasi producator.

Nota: „ Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt mentionate doar pentru identificarea cu usurinta a tipului de produs si NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificatii vor fi considerate ca avand mentiunea de «sau echivalent»”. Echipamentele de tip router si switch trebuie sa fie produse de acelasi producator pentru a evita problemele de interconectare.

5.2 Dezvoltare sistem de comunicatii securizate de backup pentru dispecerate

Cerinte privind caracteristici generale ale solutiei, arhitectura de sistem și reziliența geografică

Solutie redundanta cu disponibilitate permanenta a serviciilor:

Sistemul va fi compus din două unități centrale de gestiune a apelurilor, configurate în regim High Availability (HA) distribuit geografic, doua echipamente de conectare cu rețeaua TDM (fiecare cu cate doua interfete ISDN E1 PRI) in fiecare dispecerat si 15 posturi de comunicatie dispecer, fiecare inzestrat cu terminal telefonic si client software de comunicatie unificata.

Solutia instalata in cele două locații trebuie să funcționeze ca un singur sistem logic. În cazul în care o locatie devine indisponibilă, locația functionala preia automat toți cei 30 de agenți.

Sincronizare: replicarea bazei de date de audit (CDR) și a înregistrărilor audio (Call Recording) trebuie să se facă în timp real între cele două locații prin conexiunile de date (infrastructura de rețea Ethernet).

Cerințe de rețea și conectivitate: solutia trebuie să permită funcționarea în locații fizice diferite și în segmente de rețea distincte, suportând rutarea prin echipamentele de interconectare cu rețeaua TDM implicate diferite și planuri de adresare IP diferite.

Mecanisme de sincronizare: sincronizarea în timp real, prin conexiunea de trafic de date Ethernet, a bazei de

CAIET DE SARCINI

date de configurare, a mesajelor vocale (voicemail), a jurnalelor detaliate de apeluri (CDR) și a înregistrărilor audio ale apelurilor între cele două locații.

Justificare tehnică: Spre deosebire de soluțiile cu redundanță locală - instalate în același segment de rețea - arhitectura distribuită geografic este obligatorie pentru dispeceratele cu funcționare critică și transformă întregul sistem dintr-o soluție simplă de telefonie într-o infrastructură de importanță critică.

Aceasta garantează redundanța totală a datelor și a serviciului în cazul pierderii complete a unui centru de date, asigurând că înregistrările sunt replicate instantaneu la distanță, eliminând riscul pierderii dovezilor audio în cazul unui incident major la unul dintre sedii.

Subsistem de monitorizare, audit și integrări software:

Audit și retenție: jurnalizare completă a apelurilor (Call Detail Records - CDR) și înregistrare audio cu retenție pe stocarea internă pentru minim 6 luni. Sistemul va permite arhivarea automată către resurse externe (NAS, server FTP).

Raportare avansată: Motor grafic integrat pentru generarea rapoartelor de tip SLA (Service Level Agreement), statistici pe cozi de așteptare (rata de abandon, timp mediu de așteptare) și performanță individuală agenți (Talk Time, Idle Time). Programare pentru trimitere automată pe email în formate PDF/CSV.

Funcții integrate de comunicare (UC): Licențiere inclusă pentru aplicații client de comunicare integrată (Windows, macOS, iOS, Android) care suportă apeluri video/audio, chat, prezență și fax electronic.

Integrare software (CRM/MS Teams): Conectori integrați pentru Microsoft Dynamics, Oracle Sales Cloud și integrare directă pentru fluxul de voce în Microsoft Teams. Suport pentru sincronizarea directoarelor prin LDAP/Active Directory și autentificare de tip Single Sign-On (SSO).

Securitate: Protecție integrată împotriva atacurilor de tip DoS (Denial of Service) și Brute Force asupra protocolului SIP.

Model de licențiere și sustenabilitate:

Pentru a asigura sustenabilitatea proiectului și controlul costurilor, eventuala activare prin chei de licență a funcționalităților soluției oferite va fi structurată astfel:

Licențierea funcționalităților de bază: Licențele pentru extensiile (posturile) de interior și funcțiile de bază IP-PBX (apelare, transfer, parcare, voicemail) trebuie să fie de tip PERPETUU (Permanent License). Odată achiziționate, acestea nu trebuie să expire sau să necesite taxe de subscripție pentru funcționarea de bază a sistemului de voce.

Licențierea serviciilor avansate: Doar funcționalitățile extinse de gestiune, monitorizare și raportare a dispecerizării apelurilor (Call Center) și actualizările de securitate pot fi oferite sub formă de subscripție anuală.

Independența funcțională: Expirarea subscripțiilor de servicii avansate NU trebuie să afecteze capacitatea sistemului de a primi sau efectua apeluri de voce de pe terminalele telefonice fizice sau software sau funcționarea trunk-urilor E1/SIP.

În cazul unor constrângeri bugetare viitoare care ar împiedica reînnoirea subscripțiilor, dispeceratul trebuie să rămână operațional la nivelul funcțiilor de bază de voce (funcționalități critice), pierzând doar facilitățile de mobilitate și raportare avansată, nu și capacitatea de comunicare.

Licențierea funcționalităților de bază se va aplica exclusiv asupra unităților centrale de control a sistemului (echipamente fizice instalate local).

Orice ofertă care propune un model de tip "Voice-as-a-Service" integral (unde telefoanele nu mai pot iniția sau recepționa apelurile la sistarea serviciilor de tip subscripție), cu furnizarea serviciilor de configurare, gestiune, monitorizare și raportare din infrastructura de cloud public sau privat a producătorului va fi considerată neconformă, deoarece nu îndeplinește cerința de independență a funcțiilor critice de voce.

Unitatea centrală de gestiune a apelurilor, terminalelor, planurilor de numerotare, schemelor ierarhice de direcționare a apelurilor, cu funcții de monitorizare în timp real, înregistrare a apelurilor și raportare extinsă

Tipul platformei: Echipament specializat, destinat exclusiv rularii serviciilor solicitate pe o arhitectură hardware dedicată, cu sistem de operare securizat (hardened OS), optimizat pentru procesare de semnalizări și comunicații de voce peste infrastructura de date (VoIP).

Format fizic și posibilități de montaj: Carcasă metalică robustă, format standard 1U Rack-mountable (conform EIA-TIA-310D), incluzând kit-ul complet de montaj în rack de 19 inch.

Redundanță la nivel de alimentare: Surse de alimentare duale (1+1), cu o putere de maxim 750W fiecare, pentru a permite înlocuirea unei surse fără oprirea sistemului.

Arhitectură hardware internă: dedicată pentru procesarea traficului de voce peste infrastructura de rețea de date (VoIP)

Stocare și protecție date: Minimum 2 unități de stocare interne de 1TB fiecare (capacitate brută de stocare 2TB), configurabile în RAID 1, cu posibilitatea parametrizării dimensiunii spațiului de stocare destinat înregistrărilor convorbirilor.

Ofertantii vor prezenta indicatorii orientativi pentru dimensionarea spațiului de stocare destinat înregistrării convorbirilor, în funcție de algoritmul de compresie pentru arhivare.

Capacități nominale de sistem:

Mecanism de comutare (failover): Detectare automată a erorilor pe interfețe (Port Monitoring) și servicii (HTTP/SIP monitoring)

Număr minim extensii (posturi de lucru cu adresare IP și extensii alocabile) licențiate: minimum 2000 de utilizatori (extensii).

Număr minim de apeluri concurente (simultane) prelucrate: minimum 300 de apeluri (SIPS/RTP).

Număr minim de canale SIP trunk simultane: 100

Capacitate de înregistrare simultană (call recording) pentru minim 150 de fluxuri audio.

Capacitate de instantiere teleconferințe audio: minimum 20 teleconferințe simultane

Număr de participanți teleconferințe audio: minimum 20 per teleconferință

Interfețe de rețea:

- minimum 4 interfețe 10/100/1000Base-T (RJ45), cu posibilitate de configurare a conexiunilor agregate

- funcții implementate de aplicare automată a unor indicatori de priorizare în rețea a traficului voce și video: obligatorii

- sistem de raportare grafică integrat, capabil să genereze statistici detaliate pe cozi de așteptare, performanță agenți și timpi de răspuns, cu export automat pe email.

Funcționalități gestiune a dispecerizării apelurilor:

- implementare gestiune a cozilor de apeluri (call queues), configurare grupuri de agenți, rutare bazată pe competențe (skill-based routing), și rapoarte detaliate (CDR/SMDR), cu un minimum de 10 agenți concurenți activi.

- înregistrare apeluri (Call Recording), parcare apeluri (Call Parking), conferințe multi-parti (Conference Bridges), și funcția "Follow-Me"

Funcționalități unificate de comunicație și integrare cu ecosisteme terțe:

- client software de comunicație integrat: Licențiere inclusă pentru aplicații de desktop (Windows/macOS) și mobil (iOS/Android) care să permită chat, prezență, fax electronic și control apel.

- Microsoft Teams: Integrare nativă pentru utilizarea infrastructurii de voce în interiorul interfeței Microsoft Teams (via Direct Routing sau aplicație dedicată).

Justificare tehnică: Integrarea cu MS Teams și disponibilitatea clientului software asigură flexibilitatea operării de la distanță în regim de "Business Continuity Plan", transformând orice calculator sau smartphone într-un post de dispecer complet securizat.

- Integrare CRM: Suport nativ (fără să necesite dezvoltări software) pentru Microsoft Dynamics, Oracle Sales Cloud și alte platforme via API/Websocket.

- Sincronizare LDAP/Active Directory: Pentru importul utilizatorilor și autentificare de tip Single Sign-On (SSO).

Gestionarea Apelurilor:

- Auto-Attendant (IVR): Suport pentru meniuri vocale multi-nivel, configurabile pe intervale orare și sărbători și rutare inteligentă a apelurilor

- Grupuri de apel (Hunt Groups): Strategii de apel configurabile (simultan, secvențial, circular).

- Call Recording: Înregistrare centralizată a apelurilor cu posibilitate de stocare locală sau pe servere externe (FTP/NFS).

- Posibilitatea transcrierii mesajelor audio (voice mails) si a inregistrarilor audio folosind un motor text-to-speech dezvoltat de catre producator
- Conferință Video/Audio: Bridge de conferință integrat, cu suport pentru partajarea ecranului (screen sharing) și chat.
- Posibilitatea interventiei in apel a supervisorului (sef tura dispecerat)
- Mesagerie și notificări:
- Voicemail-to-Email: Trimiterea mesajelor vocale ca fișiere atașate (.wav) către adresa de e-mail a utilizatorului.
- Fax-to-Email: Conversia faxurilor primite în format PDF și livrarea acestora pe e-mail.
- Interfață Self-Service: Portal web pentru utilizatori finali unde aceștia își pot gestiona setările de redirecționare, mesajele vocale și agenda personală.
- Securitate comunicații:
- Criptarea semnalizării și a fluxului de voce utilizând protocoalele TLS (Transport Layer Security) și SRTP (Secure Real-time Transport Protocol).
- Protecție integrată împotriva atacurilor de tip DoS (Denial of Service) și Brute Force asupra protocolului SIP.
- politici de parolare și auditare
- Management centralizat:
- Consolă de administrare cu interfata accesibila prin browser web (HTTPS) cu tablouri de bord în timp real pentru monitorizarea sistemului.
- Auto-provisioning: Descoperirea automată și configurarea centralizată a telefoanelor IP (zero-touch deployment).
- Sistem avansat de raportare și logare a apelurilor (Call Detail Records - CDR).
- Functii de auditare a parolelor: obligatorii
- Gestiunea accesului la functii administrative bazata pe definirea rolurilor de operator: obligatorie
- Servicii Hardware si Suport:
- 3 ani 24x7 cu timp de raspuns de 4 ore.
- Subsistem de raportare:
- solutia trebuie să implementeze un motor de raportare integrat, capabil să genereze statistici detaliate fără a necesita baze de date externe.
- Tipuri de rapoarte obligatorii configurabile:
- Raport statistici cozi de asteptare apeluri (Queue Statistics): Timpul mediu de așteptare, numărul de apeluri preluate vs. apeluri abandonate, rata de abandon.
- Raport performanță agenți (Agent Statistics): Durata totala de activitate (sesiune de lucru), durata de inactivitate intre apeluri, durata conversatii aple (Talk Time), număr de apeluri per agent.
- Raport nivel de indeplinire a parametrilor serviciului (SLA): Procentul de apeluri preluate în pragul de timp predefinit (ex: 80% din apeluri preluate sub 20 secunde).
- Raport distribuție apeluri: Analiză pe ore, zile și luni pentru dimensionarea corectă a turelor de dispeceri.
- Managementul rapoartelor:
- Programare automată: Posibilitatea de a trimite rapoartele automat pe email (PDF/CSV) la intervale zilnice, săptămânale sau lunare.
- Dashboard în timp real: Panou de control grafic pentru supervisor, care afișează numărul de apeluri în așteptare și starea curentă a fiecărui agent.
- Audit (CDR): Jurnalizare completă (Call Detail Records) cu posibilitate de filtrare după departament, prefix, durată sau cost.
- Justificare Tehnică: Monitorizarea SLA-ului și a ratei de abandon este o cerință operațională pentru a garanta că dispeceratul răspunde în timpii optimi solicitărilor.
- Raportarea automată pe email asigură transparența activității către management, fără intervenția manuală a operatorilor IT.

Gateway-uri de interconectare TDM-IP (E1/PRI)

Se vor furniza câte 2 unități gateway fizice independente per locație, destinate conversiei între trunchiurile digitale furnizate de operatorii telecom și infrastructura VoIP.

Format fizic și posibilitati de montaj: Carcasă metalică robustă, format standard 1U Rack-mountable (conform EIA-TIA-310D), incluzând kit-ul complet de montaj în rack de 19 inch.

Interfețe digitale: Minim 2 porturi fizice ISDN E1/PRI G.703 120 ohmi balanced, cu implementarea interpretării corecte a formatului ETSI Caller ID per unitate gateway.

Redundanță rețea (Dual LAN): Minim 2 porturi Gigabit Ethernet (10/100/1000 Mbps) RJ45 per unitate, configurabile pentru redundanță la nivel de conexiune și cu posibilitati de configurare a segmentarii de trafic (VLANs)

Support protocoale semnalizare: Implementare ISDN PRI E1, R2 și SIP (conform RFC 3261).

Codec-uri implementate pentru procesare trafic de voce și video: Audio: G.711 μ -law/A-law, G.729a, G.722, Opus - Video: H.263, H.264

Servicii de fax: Implementare nativă a protocolului T.38 (Fax over IP) pentru a asigura interoperabilitatea cu echipamentele fax tradiționale prin trunchiuri SIP.

Functii auxiliare: DTMF, implementare conforma cu RFC2883

Securitatea comunicațiilor: Criptarea obligatorie a semnalizării și a fluxului de voce între gateway și unitatea centrală utilizând protocoalele TLS (Transport Layer Security) și SRTP (Secure Real-time Transport Protocol).

Management integrat: Descoperirea automată (Auto-discovery) și configurarea centralizată din consola unității centrale. Modificările de securitate și rutare trebuie să fie propagate automat, fără a necesita accesarea unei interfețe web separate pentru operarea de zi cu zi a gateway-urilor.

Terminale IP profesionale pentru dispeceri cu caracteristici ergonomice adaptate operării în regim de dispecerat

Sistem vizual: Ecran LCD color cu diagonală de minim 4 inches (480 x 272 pixeli), cu iluminare de fundal și senzor de iluminare ambientală pentru ajustarea automată a luminozității în medii de dispecerat cu lumină controlată.

Interfață de operare și productivitate:

Minim 10 taste fizice programabile, fiecare dotată cu LED-uri bicolore pentru monitorizarea stării extensiilor.

Support pentru paginare digitală a afisajului (minim 3 pagini), permițând programarea a minim 25 de funcții (linii, speed-dial, servicii).

Conectivitate avansată:

Bluetooth integrat (v4.0 sau superior): Support nativ pentru conectarea căștilor wireless profesionale fără ocuparea portului USB și fără adaptoare externe.

Switch Gigabit integrat cu 2 porturi (10/100/1000 Mbps) cu suport PoE (Power over Ethernet) Class 3 (consum <10W).

Minim 1 port USB 2.0 pentru accesorii.

Justificare Tehnică: În regim de dispecerat, operatorul trebuie să poată vedea dintr-o privire cine este disponibil în teren sau în alte departamente.

Cele 10 taste fizice bicolore reduc timpul de căutare în agendă. Bluetooth-ul integrat este o cerință de securitate a muncii și ergonomie, permițând dispecerului să se deplaseze în proximitatea postului fără a părăsi apelul, eliminând totodată riscul de rupere a cablurilor sau a conectorilor mecanici prin utilizarea căștilor cu fir.

Calitate audio și procesare: Support pentru codecuri HD (G.722) pe toate căile (receptor, difuzor, cască), cu funcție de atenuare acustică a ecoului (Acoustic Echo Cancellation) Full Duplex.

Toate componentele soluției trebuie să fie de la același producător.

Nota: „ Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt

mentionate doar pentru identificarea cu usurinta a tipului de produs si NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificatii vor fi considerate ca avand mentiunea de «sau echivalent». Echipamentele de tip router si switch trebuie sa fie produse de acelasi producator pentru a evita problemele de interconectare.

5.3 Dezvoltare sistem management incidente

Nr. crt	Descriere generala	livrabil
Caracteristici Generale		
1	Solutia permite gestionarea activelor IT, a activitatilor de Help Desk, cat si a aplicatiilor specifice activitatii de Management de Proiect bazate pe standardul ITIL;	DA
2	Solutia permite acces bazat pe interfata web	DA
3	Solutia permite crearea unor campuri de urmarire personalizate	DA
4	Solutia oferita este ITIL Ready	DA
5	Solutia permite configurari ("Configuration wizard"), bazata pe fluxuri predefinite	DA
Gestionarea activelor IT -Asset Management		
6	Solutia permite descoperirea automata a statiilor de lucru din retea;	DA
7	Solutia permite descoperirea tuturor dispozitivelor IP, cum ar fi imprimare, scannere, etc;	DA
8	Solutia permite scanarea completa a statiilor Windows, Linux si MAC;	DA
9	Solutia permite descoperire bazata, atat cu agenti, cat si fara;	DA
10	Solutia permite scanarea distribuita a statiilor de lucru;	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
11	Solutia permite asocierea informatiilor legate de existent si producator	DA
12	Solutia asigura Istoricul inventariilor anterioare impreuna cu cererea aferenta;	DA
13	Solutia asigura complianta software	DA
14	Solutia asigura gestionarea licentelor software;	DA
15	Solutia asigura gestionarea acceptantelor software;	DA
16	Solutia permite configurarea informatiilor privind amortizarea inventarului;	DA
17	Solutia permite realizarea graficelor de relationare intre inventarii, statii de lucru, software si utilizatori ;	DA
Gestionarea contractelor		
18	Solutia asigura crearea si gestionarea contractelor;	DA
19	Solutia permite adaugarea de informatii si atasarea de documente legate de contract	DA
20	Solutia permite asocierea contractelor la Inventare;	DA
21	Solutia permite generarea alarme inaintea expirarii contractelor	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
22	Solutia permite urmarirea contractelor reinoite	DA
Gestionarea achizitiilor		
23	Solutia permite gestionarea cererilor de achizitie	DA
24	Solutia permite contactare pro ducator/ distribuitor/vanzator direct din aplicatie;	DA
25	Solutia permite facilitati de integrare intre achizitie, inventar si producator	DA
26	Solutia are inclus sistem de aprobare a achizitiilor;	DA
Standarde ITIL Suportate		
27	Solutia asigura gestionarea incidentelor ("Incident Management");	DA
28	Solutia asigura gestionarea problemelor ("Problem Mana gement");	DA
29	Solutia asigura gestionarea Schimbarilor ("Change Management");	DA
30	Solutia are inclus modul pentru Project Management;	DA
31	Solutia are inclusa Baza de date integrate ("CMDB – Configuration Management Database	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
32	Solutia are inclus Catalog de servicii ("Service Catalogs");	DA
Gestionarea apelurilor si cererilor		
33	Permite generarea cererilor prin:Email, Telefon, Portal	DA
35	Solutia asigura depozit central pentru stocarea si urmarirea situatiilor	DA
36	Solutia permite generare automata de tichete;	DA
37	Solutia asigura afisare pe monitor catre utilizatori a situatiilor importante	DA
38	Solutia permite receptionare si transmitere mesaje email din aplicatie	DA
39	Solutia permite receptionare si transmitere mesaje SMS din aplicatie	DA
40	Solutia permite creare tichete din mesajele de email primite;	DA
41	Solutia permite clasificarea si rutarea automata a mesjelor	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
42	Solutia permite redirectarea cererilor in mod automat si manual;	DA
43	Solutia permite personalizarea formei de cereri;	DA
44	Solutia asigura inclus editor de text avansat cu posibilitatea adaugarii de atasamente	DA
45	Solutia permite programarea cererilor	DA
46	Solutia permite calendar pentru tehnicieni;	DA
47	Solutia asigura acces bazat pe roluri pentru Tehnicieni;	DA
48	Solutia permite crearea de activitati multiple pentru o cerere	DA
49	Solutia permite tratarea activitatilor dependente;	DA
50	Solutia are inclus Email Spam Filter & Email Notification Filter	DA
51	Solutia permite clasificare si rutarea cererilor bazate pe grupuri de lucru;	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
52	Solutia are incluse functionalitati de accesare rapida si inistoric de acces la nivel de interfata utilizator;	DA
53	Solutia permite clasificarea cererilor bazata pe categorii;	DA
54	Solutia permite comunicarea prioritatilor si a severitatilor o data cu cererea;	DA
56	Solutia permite activarea unui mesaj de email in momentul aparitiei unui eveniment prevazut intr-o regula de business;	DA
57	Solutia permite aplicarea unei reguli de business dupa editarea unei cereri;	DA
58	Solutia permite continuarea cu o sub-regula de business dupa ce a fast gasita o regula;	DA
59	Solutia permite gestionarea eficienta a tehnicienilor bazata pe cozi de suport;	DA
60	Solutia permite atasarea de documente la o cerere;	DA
61		DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
	Solutia permite gestionarea, editarea, asignarea si inchiderea de grupuri de tichete;	
62	Solutia asigura liste de ordine pentru distribuirea tehnicienilor de service si mentenanta;	DA
63	Solutia permite implementare reguli de inchidere a cererilor;	DA
Gestionarea incidentelor		
64	Solutia permite clasificarea incidentelor	DA
66	Solutia permite atasarea de informatii legate de: Impact, Urgenta, Prioritate, Matrici de prioritate, Stare (ex. Open, On hold, Closed, etc.);	DA
67	Solutia asigura posibilitate de a lega un incident de un email ("Mailbox Management");	DA
68	Solutia permite Posibilitate crearea de template -uri de incidente;	DA
Catalog de servicii		
69	Solutia permite afisarea serviciilor disponibile;	DA
70	Solutia permite implementarea de template -uri pentru cereri de service;	DA
71	Solutia are incluse fluxuri de lucru pre-configurate;	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
72	Solutia permite procese de aprobare in mai multe faze;	DA
73	Solutia permite configurarea de SLA - Service Level Agreement - asumat in timp;	DA
74	Solutia permite adaugarea de Categori de Servicii, Resurse si Servicii;	DA
75	Solutia permite asocierea de multiple activitati dependente la un Template	DA
Functionalitatea Self Service		
76	Solutia are inclus un portal Self-service de tip web-based inclus in aplicatie;	DA
77	Solutia permite crearea de cereri pentru utilizatorii finali;	DA
78	Solutia permite verificarea si actualizarea starii unei cereri existente;	DA
79	Solutia permite actualizarea detaliilor aferente contactelor;	DA
80	Solutia permite cautarea in baza de cunostine pentru utilizatori;	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
81	Solutia are inclusa o sectiune de tip "Frequently Asked Questions (FAQs)";	DA
82	Solutia permite actiuni de aprobare;	DA
Gestionarea bazei de cunostiinte (Knowledge base)		
83	Solutia permite tehnicienilor acces la un serviciu de gestionare a bazei de cunostiinte;	DA
84	Solutia permite adaugarea de solutii dupa aprobare;	DA
85	Solutia permite cuvinte cheie pentru gasirea solutiilor pe baza informatiilor din cerere;	DA
86	Solutia permite indexarea cautarilor de documente pentru obtinrea unor rezultate in mod rapid;	DA
87	Solutia permite pastrare instoricului de cautari;	DA
88	Solutia are inclusa functionalitatea Frequently Asked Questions (FAQs);	DA
89	Solutia are editor de text integrat;	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
Gestionarea problemelor		
90	Solutia permite detectarea si clasificarea problemelor;	DA
91	Solutia permite initierea unei probleme noi dintr-un incident;	DA
92	Solutia permite Initierea/ Inregistrarea unei probleme noi;	DA
93	Solutia permite asocierea unor incidente multiple intr-o singura problema;	DA
94	Solutia permite prioritizarea problemelor;	DA
95	Solutia permite adaugarea de informatii legate de cauze initiale, impact, etc.;	DA
96	Solutia permite adaugare de solutii temporare, solutii sau erori cunoscute;	DA
97	Solutia permite inchiderea problemelor;	DA
Gestionarea schimbarilor		
98	Solutia permite Initierea /Inregistrarea de noi cereri de schimbare;	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
99	Solutia permite initierea de cereri de schimbare din incidente /probleme;	DA
100	Solutia permite asociere a unor incidente/ probleme multiple la o schimbare;	DA
101	Solutia permite creare a unui comitet de aprobare a schimbarilor ("Change Advisory Boards (CABs)");	DA
102	Solutia permite trimiterea spre aprobare a cererilor de schimbare catre membrii CAB;	DA
103	Solutia permite adaugarea de informatii legate de analiza impactului, cauze, simptome;	DA
104	Solutia permite inregist rarea solutiilor permanente si temporare;	DA
105	Solutia permite facilitati de coordonare a implementrii schimbarii;	DA
106	Solutia permite trimiterea spre reverificare a schimbarilor;	DA
107	Solutia permite trimierea de anunturi catre tehnicieni si /sau utilizatori finali;	DA
Project Management		
108	Solutia permite integrarea de Proiecte, Milestones- uri si Task- uri;	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
109	Solutia permite gestionarea si planificare task - urilor;	DA
110	Solutia permite pastrarea istoricului unui proiect;	DA
111	Solutia permite estimarea efortului;	DA
112	Solutia permite notificari si comentarii;	DA
113	Solutia permite gestionarea timpului;	DA
114	Solutia permite realizarea de diagrame Gantt;	DA
115	Solutia permite o harta de privire generala a Proiectului;	DA
Gestionare SLA		
116	Solutia permite configurare de nivele diferite de escaladare;	DA
117	Solutia permite escaladari automate pe timpul perioadei de escaladare	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
118	Solutia permite notificare inainte de expirare SLA;	DA
Raportare		
119	Solutia are incluse rapoarte standard pre-definite;	DA
120	Solutia permite realizarea de rapoarte personificate in format tabelar;	DA
121	Solutia are incluse unelte de creare interogari pentru rapoarte ("Query Builder");	DA
122	Solutia permite integrare cu aplicatii de raportare profesionale;	DA
123	Solutia permite salvare rapoarte in format .csv, .xls si Pdf;	DA
124	Solutia permite generarea si ditribuirea automata a rapoartelor ("Reports Scheduler");	DA
125	Solutia permite analiza a evolutiei si performantelor;	DA
126	Solutia permite actualizarea in timp real a rapoart elor;	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
127	Solutia permite salvarea si programarea a rapoartelor customizate;	DA
Cerinte de integrare		
128	Solutia permite Integrare cu LDAP, Active Directory(AD)	DA
129	Solutia permite integrarea cu sisteme de email si SMS;	DA
130	Solutia are incluse aplicatii pentru dispozitive iPhone si Android;	DA
131	Solutia are Interfata de integrare cu sisteme de tip computer telephony (CTI)	DA
132	Solutia permite utilizarea serviciilor web;	DA
133	Solutia permite integrare API	DA
134	Solutia permite importarea utilizatorilor si drepturi din Microsoft Active Directory	DA

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
135	Solutia permite importuri programate din Microsoft Active Directory	DA
Release management		
136	Solutia permite crearea de sabloane de lansare versiuni, roluri si stari personalizate.	DA
137	Solutia permite construirea de fluxuri de lucru de lansare versiuni	DA
138	Solutia permite configurarea etapelor, starilor si tranzitiilor pentru fiecare flux de lucru	DA
139	Solutia permite creare planuri de impact, lansare, de retragere si liste de verificare pentru implementare.	DA
140	Solutia permite desfasurarea instruirii si revizuirii post-deployment	DA
141	Solutia permite trimiterea de anunturi pentru downtime planificat din modulul de lansare	DA
Cerinte tehnice		
142	Solutia trebuie sa suporte urmatoarele sisteme de operare:	DA
	-Linux	
	-Windows	
143	Solutia trebuie sa suporte urmatoarele baze de date:	DA
	• SQL	
	• MYSQL	
	Postgres	

CAIET DE SARCINI

Nr. crt	Descriere generala	livrabil
144	Solutia trebuie sa suporte urmatoarele browsere	DA
	<ul style="list-style-type: none">• Microsoft Edge	
	<ul style="list-style-type: none">• Firefox	
	<ul style="list-style-type: none">• Chrome	
Platforma de instalare		
145	Implementarea proceselor ITIL pentru a imbunatati eficienta si eficacitatea operatiunilor IT, gestionarea schimbarilor;	DA
146	Planificarea proiectelor: Definirea obiectivelor, domeniului de aplicare, programului proiectelor si urmarirea lor;	DA
147	Asigurarea cerintelor pentru indeplinirea conformitatii cu standardele (GDPR, HIPAA, GLBA, FISMA, ISO 27001).	DA
148	Protectie a activelor IT impotriva accesului neautorizat;	DA
149	Alertare proactiva cu privire la licentele care urmeaza sa expire sau care sunt pe cale de a expira;	DA
150	Primirea, urmarirea si rezolvarea solicitarilor de asistenta	DA
151	Solutia software va rula pe masini virtuale puse la dispozitie de autoritatea contractanta	DA
152	Solutia trebuie sa aibe interfata in limba romana nativ si sa fie licentiata pentru 60 tehnicieni 3000 noduri cu servicii de asistenta de la producator 24/7 pentru 36 luni.	DA
153	Solutia trebuie sa vina dotat cu 8 clustere de NVIDIA DGX Spark pentru analiza incidentelor si 4 monitoare WQHD HP Series 7 Pro de 34 inchi – 734pm	DA
153	Solutia trebuie sa poata rula pe cel putin urmatoarele sisteme de operare: Windows 2016 si mai nou, Red Hat Linux 7.2 sau mai nou, Linux Debian 3,0 sau mai nou	DA
154	Solutia trebuie sa poata rula pe cel putin urmatoarele baze de date: MySQL 4.1.8 sau mai nou, MS SQL 2000 sau mai nou	DA

Nota: „ Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt mentionate doar pentru identificarea cu usurinta a tipului de produs si NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificatii vor fi considerate ca avand mentiunea de «sau echivalent»”. Echipamentele de tip router si switch trebuie sa fie produse de acelasi producator pentru a evita problemele de interconectare.

5.4 Dezvoltare Solutie Load Balancer

Solutia ofertata trebuie sa ofere:

- Configuratie: HA Pair (Active/Standby sau Active/Active)
- Licenta: 64K Layer 7
- Form factor: Appliance hardware dedicat
- Minim doua clustere
- Servicii de asistenta 24x7 cu timp de raspuns 2 ore de la producator pentru 36 de luni
- Update-uri software si patch-uri de securitate
- Rack kit si accesorii
- Upgrade hardware fara downtime

Arhitectura HA obligatorie cluster.

Doua appliance-uri fizice identice fiecare echopate cu cate cel putin:

- 4 interfete de 10 Gbps SFP+
- 6 interfete 10/100/1000 Mbps RJ 45
- 2 surse de alimentare redundante

Acestea trebuie sa ofere urmatoarele functionalitati:

- Sincronizare configuratie intre noduri
- Sincronizare persistenta sesiuni
- VRRP pentru failover automat
- Health-check-uri HTTPS
- Route announcement catre routere externe
- Failover transparent pentru clienti
- Graceful shutdown al backend-urilor
- Overload protection
- Failover regional prin mecanisme GSLB
- Sincronizare securizata a configuratiilor prin VPN criptat
- Detectie automata a degradarii serviciilor si rerutare trafic
- Performanta minima per appliance
- Layer 7 Proxy
- HTTPS 1.1
- Minim: 286,000 req/s
- Minim: 25.2 Gbps throughput
- HTTPS 2.0
- Minim: 321,000 req/s
- Minim: 13.7 Gbps throughput
- New TLS Keys pe secunda
- RSA 2048 minim: 9,300
- ECDSA 256 minim: 35,100
- Layer 4 Load Balancing
- Conexiuni noi pe seunda (DNAT) minim: 1,100,000
- Conexiuni noi pe seunda sec (DSR) minim: 1,200,000
- Protectie DDoS – Packet Filtering
- TCP packet flood: minim 32.2 milioane pps
- Pachete invalide: minim 39 milioane pps
- Conexiuni L7 HTTP pe secunda minim: 64,000
- Conexiuni L7 concurente minim: 160,000

- SSL TPS (TLS 1.3) minim: 16,000
- Conexiuni L4 pe secunda minim: 200,000
- Functionalitati Load Balancing
- Suport Layer 4 si Layer 7
- Suport extins pentru HTTP/1.x, HTTP/2, HTTP/3/QUIC, UDP, gRPC, MQTT, FastCGI
- Content switching Layer 7
- Suport pentru TCP si UDP
- Cookie persistence
- TLS termination si offloading
- IPv6 ready
- Direct Server Return
- Transparent proxy si NAT
- Algoritmi multipli de distribuire trafic
- WebSockets
- URL redirect
- Global Server Load Balancing
- Geo load balancing cu HTTPS health checks
- Rate limiting per client si per endpoint
- Routing bazat pe starea aplicatiilor
- VIP-less deployment options
- Management & Administrare
- Interfata Web grafica pentru administrare
- CLI dedicat
- API REST pentru automatizare
- VLAN 802.1Q
- Transparent proxy
- Bridging & bonding NIC
- VPN criptat pentru sincronizare configuratii (ChaCha20)
- Syslog, SNMP, VRRP, NTP
- SSH si serial
- Scriptable configuration
- Configuration templates si wizards
- SSL certificate lifecycle management
- Diagnostic tools integrate
- Monitoring in timp real
- Observabilitate trafic, conexiuni si backend-uri
- Jurnale detaliate pentru audit
- Alarme configurabile pe praguri
- Management multi-nivel (admin/operator)
- Integrare CI/CD si sisteme externe
- Accelerare aplicatii
- TCP/HTTP buffering
- Control dinamic al conexiunilor catre backend
- HTTP compression
- Early connection release
- OCSP stapling automatizat
- Advanced response time reporting
- Unlimited backend servers per serviciu virtual

CAIET DE SARCINI

- Filtrare cereri inutile
- Management loguri in offload mode
- Securitate integrată
- Web Application Firewall avansat
- Bot Management
- DDoS Protection – TCP flood 32M, pachete invalide 39M
- Threat intelligence feeds
- Zero-day detection
- Politici personalizate per aplicatie

Nota: „ Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt mentionate doar pentru identificarea cu usurinta a tipului de produs si NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificatii vor fi considerate ca avand mentiunea de «sau echivalent»”. Echipamentele de tip router si switch trebuie sa fie produse de acelasi producator pentru a evita problemele de interconectare.

5.5 Dezvoltare Solutie securitate ICS

Nr.	Specificatii
Asset Inventory/ Visibility	
1	Solutia trebuie sa fie capabil sa identifice pasiv echipamentele OT, IT si IoT si sa extraga informatii detaliate despre acestea cat si traficul de date generat de acestea. Trebuie sa ofere suport pentru urmatoarele protocoalele ICS: IEC 60870-5-104, DNP3, Modbus, IEC 60870-6 (ICCP), IEC 61850, MMS.
2	Pentru protocoalele ICS specificate, solutia trebuie sa fie capabil sa extraga cel putin versiunea de firmware, informatii despre dispoziv (tip echipament, model, serial, nume, adresa ip, MAC, vendor, protocol, data flow, configuratie, etc.)
3	Solutia trebuie sa fie capabila sa ofere vizibilitate asupra dispozitivelor OT cat si comunicatiilor care nu sunt bazate pe IP (ex. Fieldbus, seriale) si sa ofere informatii despre dispozitivele conectate, inclusiv cardurile I/O, cat si a subsistemelor conectate.
4	Solutia trebuie sa fie capabila sa identifice comunicarea catre echipamentele OT din spatele unui gateway Ethernet.
5	Solutia trebuie sa identifice modificarile aparute asupra configuratiei si sa permita trimiterea de alerte in cazul in care detecteaza anomalii.
6	Sistemul trebuie să poată extrage informații despre software-ul instalat pe active bazate pe Windows prin metode pasive (pentru software critic, cum ar fi aplicații de acces la distanță, cum ar fi TeamViewer, browsere instalate) și metode active (toate programele de aplicație instalate)

CAIET DE SARCINI

Nr.	Specificatii
7	Solutia trebuie sa permita colectarea de informatii despre hardware ale unui echipament OT cat si despre perifericele conectate la acesta (ex. Stick USB) pentru echipamentele cu sistem de operare Windows.
8	Solutia trebuie sa permita utilizatorilor sa faca customizari pentru a putea colecta urmatoarele informatii din dispozitivele IOT: - Model - Versiune Firmware - Hostname - Vendor - Tip Dispozitiv - Descriere
9	Solutia trebuie sa ofere o vizibilitate granulara asupra comunicatiilor dintre dispozitivele OT/IOT din cadrul rețelei pana la nivel de comanda transmisa prin intermediul protocoalelor ICS.
10	Solutia trebuie sa ofere informatii detaliate despre traficul generat de catre dispozitivele OT/IoT cum ar fi: protocol, porturi utilizate, frecventa, cat si comanda transmisa.
11	Solutia trebuie sa catalogheze automat traficul dintre dispozitivele OT/IoT si genereze o harta cu acestea.
12	Sistemul va fi capabil să extragă valori de proces din protocoalele OT aplicabile. pentru a oferi o vedere a procesului OT cu valori care sunt citite sau scrise din activele OT inclusiv valoarea reală, registrul/eticheta implicată și funcția utilizată. Sistemul trebuie să poată alerta asupra acestor valori în afara unui interval definit de utilizator.
13	Solutia trebuie sa ofere o analiza detaliata a traficului de retea generat de catre echipamentele OT/IoT. (Ex. Protocoale utilizate, volumul de trafic generat de acestea, destinatia traficului intern sau extern.
14	Solutia trebuie sa permita oferirea de statistici detaliate despre traficul generat de catre dispozitivele OT/IoT si sa permita gruparea acestor statistici in functie de protocolul ICS folosit perioada de timp sau grupuri de dispozitive.
15	Solutia trebuie sa ofere informatii despre disponibilitatea echipamentelor OT/IoT cat si despre erorile de comunicatii aparute.
Risk and Vulnerability	
1	Solutia trebuie genereze automat o analiza cu riscuri al dispozitivelor OT/IoT luand in considerare urmatoorii factori: vulnerabilitatile echipamentelor, impactul echipamentului asupra altor echipamente, furnizarea unui singur scor de risc pentru echipamet, furnizarea de detalii pentru nota de risc acordata.

CAIET DE SARCINI

Nr.	Specificatii
2	Solutia trebuie genereze automat o analiza cu riscuri pentru grupuri virtuale de dispozitive OT/IoT luand in considerare urmatoorii factori: vulnerabilitatile echipamentelor, impactul unui echipament asupra grupului de echipamente cat si impactul grupului asupra altor grupuri de echipamente, furnizarea unui singur scor de risc pentru grupul echipamete, furnizarea de detalii pentru nota de risc acordata.
3	Solutia trebuie sa ofere un top 10 cu echipamentele ce au o nota de risc mare in interiorul infrastructurii.
4	Solutia trebuie sa catalogheze echipamentele OT/IoT esentiale in infrastructura ce au o nota de risc mare.
5	Solutia va furniza un singur indicator de risc pentru toate rețelele monitorizate.
6	Solutia trebuie furnizeze informatii despre tendintele de schimbare ale indicatorului de risc.
Segmentation	
1	Solutia trebuie sa permita gruparea automata a echipamentelor OT/IoT monitorizate in micro-segmentare ale rețelei, aceasta grupare trebuie sa fie bazata pe functia si comportamentul echipamentelor monitorizate, si sa ofere posibilitatea de ale vizualiza pe baza de: subrețele, comportamentul echipamentelor, functia echipamentelor, cat si combinatii de caracteristici.
2	Solutia trebuie sa ofere posibilitatea de a vizualiza grafic flowurile de date dintre dispozitivele OT/IoT.
3	Sistemul va permite afisarea in mod granular comunitiile intre grupurile de dispozitive OT/IoT pe baza de sabloane si va permite utilizatorului sa identifice configuratiile gresite.
4	Sistemul va genera automat politici de grup pe baza modelelor de comunicare si a functiei dispozitivelor OT/IoT, si va permite minim urmatoarele: revizuirea politicilor, validarea politicilor, customizarea politicilor.
5	Sistemul trebuie sa permita aplicarea de politici ce guverneaza grupurile de dispozitive OT/IoT si sa alerteze administratorul la incalcarea acestora.
6	Sistemul trebuie trimita fie dotat cu un sistem de autoinvatare ce permite clasificarea si gruparea dispozitivelor in zone virtuale pentru a putea defini politici bazate pe comunicatia dintre dispozitive.
7	Sistemul trebuie sa aiba capacitatea de a evidentia politicile riscante, traficul cu periculos bazat pe sabloane de trafic asociat cu un comportament similar observat la la clienti din zona de distributie a energiei electrice sau geografic, pentru a permite administratorului sa identifice politicile sau modelele de comunicare care nu respectă cele mai bune practici.
Threat Detection	

CAIET DE SARCINI

Nr.	Specificatii
1	Sistemul va detecta amenintarile cunoscute utilizand baze de date personalizate de semnături din surse recunoscute la nivel de industrie (de exemplu, SNORT, YARA). Sistemul trebuie sa permita urmatoarele: dezactivarea de semnături individuale, adaugarea de semnături customizate, adauga semnături tert.
2	Producatorul solutiei trebuie sa fie capabila sa furnizeze informatii despre amenintari in timp real pentru a actualiza semnăturile sistemului pe baza serviciilor gazduite in cloud ale producatorului.
3	Producatorul trebuie sa aiba o echipa de cercetare activa cu următoarele caracteristici: a publicat cel puțin douăzeci de vulnerabilitati în ultimul an, actualizeaza mod constant informatiile despre amenintarile cunoscute prin a micșora numărul de alerte de tip fals/pozitiv;
4	Solutia va reduce in mod continu numărul de alerte fals pozitiv pe baza actiunilor de autoinvatare si supraveghere din partea unui administrator si ii va oferi acestuia urmatoarele: posibilitatea de a aproba o semnatura specifica numai pentru un anumit dispozitiv, posibilitatea de a aproba o semnatura specifica pentru o un grup sau zona de dispozitive"
5	Solutia trebuie sa suporte si sa inteleaga comportamentul operational a a chipamentelor cel puțin pentru urmatoarele protocoale ICS: IEC 60870-5-104, DNP3, Modbus, IEC 60870-6 (ICCP), IEC 61850, MMS
6	Pentru protocoalele ICS enumerate mai sus, solutia trebuie sa aibe minim urmatoarele caracteristici: Detectare si alertare cu privire la modificarile de configurare, Detectare si alertare cu privire la schimbările de functionare, sa faca distingere intre comenzile de protocol, cum ar fi valorile de citire/scriere, descarcare/incărcare program, schimbarea modului controlerului, editarea controlerului online, actualizarea firmware-ului etc.Detectare si alertare cu privire la editările controlerelor ICS,
7	Solutia trebuie sa fie capabila sa inteleaga operatiuni de inginerie complexe, de exemplu, o operatiune de descarcare a codului nu trebuie sa fie împărțita/interpretata ca sub-comenzi de oprire, descarcare, pornire, aceasta va fi prezenta ca detectarea unei singure operatiuni de inginerie care contine toate sub-comunicatiile care au fost facute pentru a executa acea operatie de inginerie.
8	Solutia trebuie sa fie capabila sa calculeze un scor de risc granular pentru fiecare Operatiune OT identificata, pe baza contextului care se refera la retea, activele și lanțul de evenimente care au avut loc.
9	Solutia trebuie să facă distinctia între o operatiune de inginerie normala fata de un eveniment rău intentionat cu urmatorii indicatori de risc: comportament din trecut, corelare între comunicatiile dintre echipamente, modificari in sectiunea de cod, comenzi anormale.
10	Solutia trebuie sa detecteze daca o anumita operatiune de inginerie efectueaza o modificare asupra procesului/controlerului si sa afiseze toate modificarile detectate.

CAIET DE SARCINI

Nr.	Specificatii
11	Solutia trebuie sa invete din informatiile furnizate de administartor, iar solutia trebuie sa fie capabila sa utilizeze o astfel de metoda de invatare pentru a evalua rapid si usor diferenta intre functionarea normala si actiunile rau intentionate.
12	Solutia trebuie sa aibe capacitatea de a identifica pasiv anomalii in retea, cum ar fi dispozitive noi sau malitioase, comunicatii, modificari ale tiparelor de comunicare etc., pe baza unor linii de baza de Deep Packet Inspection (DPI) ale protocoalelor si comportamentul dispozitivvelor OT/IoT.
13	Soltia trebuie sa fie capabil sa evidentieze comportamentele riscante care pot fi interpretate gresit ca fiind legitime, folosind informatiile acumulate prin experientele altor clientilor din domeniul de distributie a energiei electrice si sa le evidentieze pe cele care par neobisnuite sau anormale.
14	Solutia trebuie sa permita administartorului sa personalizeze comportamentul legitim al dispozitivelor OT/IoT pentru a se potrivi cu mediul unde acestea sunt instalate.
15	Solutia trebuie sa poata corela orice actiune individuala in contextul unui lant de actiuni pentru a determina daca este neobisnuita sau prezinta un risc individual mai mare.
16	Detectarea anomaliilor trebuie sa fie asistată de corelarea dispozitive si de evaluarea riscului contextual pentru a reduce evelimentele fals pozitive.
17	Solutia trebuie sa fie capabila sa detecteze modele de comportament de securitate rau intentionate (de exemplu, atacuri man-in-the-middle).
18	Solutia trebuie sa ofere din timp alerte de securitate pentru urmatoarele activitati: interogari DNS, scanari in retea, scanari porturi, autentificari esuate.
19	Solutia trebuie sa poata distinge intre o activitate de scanare valida si o activitate de scanare rau intenționata.
20	Solutia trebuie sa poata distinge intre o conectare esuata valida si o conectare nereusita rau intentionata.
21	Solutia trebuie sa fie capabila sa detecteze noi dispozitive introduse in resea si sa faca distinctia intre dispozitivele care impun riscuri de securitate si dispozitivele care nu impun riscuri.
22	Solutia trebuie sa ofere alerte de securitate atunci cand intervin schimmbari de comportament a unui scaner de vulnerabilitati fata de cele aprobate de catre administrator.
23	Solutia trebuie sa ofere posibilitatea de a configura semnături de securitate personalizate YARA/SNORT.
24	Solutia trebuie sa ii permita administratorului sa defineasca reguli de securitate asemanatoare cu cele de pe firewall. Regulile definite trebuie sa fie granulare si nu doar pe baza de port.
Investigation	

CAIET DE SARCINI

Nr.	Specificatii
1	Solutia trebuie sa permita detectarea de amenintari bazate pe risc contextual nu doar pe tipuri de trafic sau alerte.
2	Solutia trebuie sa fie capabila sa semnalizeze indicatorii de risc cheie sau semnificativi care sa permita o înțelegere rapida a relevantei evenimentului.
3	Solutia trebuie sa fie capabila sa afiseze grafic si sa evidentieze dispozitivele într-o harta a rețelei OT legate de o alerta de amenintare. Acest lucru este pentru a permite o identificare usoara a echipamentelor afectate de catre administrator si pentru vizualizare rapida a evenimentelor care au declansat alerta.
4	Solutia trebuie sa combine si sa coreleze diferitele alerte legate de acelasi incident cibernetic si sa constuiasca o secventa de evenimente caare duc la o alerta ce permite administratorului o sortare rapida si precisa. Soluutia trebuie sa combine evenimentele conexe într-o singura notificare bazata pe urmatoarele caracteristici: dispozitiv, timp sau risk.
5	Solutia trebuie sa ofere posibilitatea de a gestiona si notifica cu usurinta admnistratorul cu informati in timp real despre modificarile aduse in retea si permita compararea modificarilor cu cele istorice. Acolo unde este cazul sa prezite diferentele dintre sectiunile de cod.
6	Solutia trebuie sa permita analiza oricaror capturi de retea de tip PCAP in mod offline si sa ofere un raport detaliat separat de datele existente in sistem.
7	Solutia trebuie sa ofere caapturi de trafic brute in format PCAP pentru evelimentele declansate ce permit analiza lor suplimentara.
Vulnerabilities	
1	Solutia pabila trebuie sa fie capabila sa afiseze toate interogariile DNS facute de catre dispozitivele OT/IoT pentru a detecta un posibil comportament malitios in retea si pentru a permite blocarea amenintarilor. Solutia trebuie sa permita identificarea interogarilor DNS pentru fiecare dispozitiv in parte pe o perioada lunnga de timp.
2	Solutia trebuie sa fie capabila sa identifice traficul extern efectuat de catre echipamentele din cadrul din cadrul infrastructurii OT/IoT.
3	Sistemul va fi capabil să realizeze o corelație completă între vulnerabilitate și activ folosind următoarele atribute: furnizor, model, firmware
4	Solutia trebuie sa fie capabila sa efectueze interogari prin WMI pentru sistemele de operare Windows si sa ofere recomandari pentru acoperirea vulnerabilitatior din retea.
5	Solutia trebuie sa detecteze in mod activ configuratiile vulnerabile ale echipamentelor pentru minim urmatoarele protocoale: FTP, SMB (v1), SMTP, SNMP (v1/v2), SSH (v1), SSL (all versions), TELNET, TFTP, TLS (1.0 – 1.1) si VNC.
6	Solutia trebuie sa detecteze echipamentele ce sunt vulnerabile la atacuri de tip DNS tunnel.

CAIET DE SARCINI

Nr.	Specificatii
7	Solutia trebuie sa detecteze dispozitivele cu sistem de operare Windows ce au mai multe placi de retea.
8	Solutia trebuie sa detecteze dispozitivele de tip ICS cu mai multe placi de retea atat activ cat si pasiv (PLCs)
9	Solutia trebuie sa identifice echipamenntele orfane ce au adrese IP si care nu trafic in retea OT/IoT.
10	Solutia trebuie sa evidentializeze traficul cu risc crescut dintre diferitele zone ale infrastructurii OT.
11	Solutia trebuie sa ofere o evidenta cu cele mai riscante cai de acces pe care un atacator le poate exploata pentru a compromite infrastructura OT sau o anumita zona.
12	Solutia trebuie sa evidentieze tipurile de trafic intre diversele subretele sau zone din cadrul inrastructurii OT/IoT.
Enterprise Readiness	
1	Solutia trebuie sa permita sa fie compatibila cu infrastructura de virtualizare existenta bazata pe tehnologie VMware si sa fie livrata sub forma de OVA.
2	Solutia va permite implementarea plug & play prin instalare si configurare asistats pas cu pas.
3	Solutia va suporta actualizari automate ale versiunilor de software dintr-o componenta gestionata centralizat, fără a fi nevoie de actualizari individuale a nodurilor de securitate.
4	Solutia trebuie sa permita actualizari centralizate pentru semnaturile de securitate si update-urile CVE.
5	Soluutia trebuie sa trimita pe e-mail atomat rapoarte cu evelimentele cheie descoperite in frastructura OT/IoT. (Exemplu: recomandaari de update-uri, interogari DNS malitioase, etc.)
6	Solutia trebuie sa expuna o interfata API ce permite integrarea cu apliatii terte.
7	Solutia trebue sa ofere un plug-in pentru intrarea in SIEM-ul existent. (Splunnk)
8	Solutia trebuie sa trimita criptat notificarile catre echipa ce se ocupa de monitorizarea atacurilor cibernetice.
9	Soltia trebuie sa permita integrarea nativa in solutia SIEM existenta. (Splunk)
10	Solutia trebuie sa permita integrarea cu solutia de control acces in retea existenta. (Cisco ISE)
11	Solutia trebuie sa permita integrarea cu solutia de securitate existenta (Checkpoint), sa o foloseasca ca senzori pentru colectarea de date si sa beneficieze de suport unificat din partea echipei TAC.

CAIET DE SARCINI

Nr.	Specificatii
12	Solutia oferata trebuie sa fie compusa din: - O consola de management ce se integreaza nativ cu Checkpoint SmartConsole ce permite gestionarea unui numar nelimitat de site-uri. - 5000 de licente pentru administrarea si monitorizarea dispozitivelor OT/IoT cu capabilitati Continuous Threa Detection
13	Solutia trebuie sa beneficieze de suport pentru o perioada de 3 ani din partea producatorului si suport unificat in portalul de suport.
14	Solutia trebuie sa se integreze nativ in solutia existenta Claroty
15	Solutia oferata trebuie sa se integreze nativ cu solutia de securitate Checkpoint si sa fie capabila sa defineasca politici de securitate automat pentru a preveni atacurile cibernetice.
16	Solutia trebuie sa suporte implementari bazate pe o arhitectura cu noduri distribuite.
17	Sistemul de monitorizare va face parte dintr-o platformă tehnologică extensibilă dezvoltată de un furnizor comun pentru a sprijini accesul securizat la activele OT critice de la distanță pentru a oferi un TCO mai mic. Modulul de monitorizare/detecție a amenințărilor va fi integrat cu modulul securizat de acces la distanță ca parte a unei platforme unificate de securitate cibernetică.
18	Solutia trebuie sa utilizeze infrastructura de securitate existenta ca senzori pentru colectarea datelor bazata pe tehnologie Checkpoint.
19	Solutia trebuie sa ofere functionalitatea de REST API ce permite integrarea cu echipamentele de securitate existente in infrastructura (Checkpoint)

Nota: „ Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt mentionate doar pentru identificarea cu usurinta a tipului de produs si NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificatii vor fi considerate ca avand mentiunea de «sau echivalent»”. Echipamentele de tip router si switch trebuie sa fie produse de acelasi producator pentru a evita problemele de interconectare.

5.6 Dezvoltare solutie de autentificare si autorizare protaluri web

Solutia trebuie sa fie compatibila cu:

- Red Hat Enterprise Linux
- OpenShift Container Platform (daca se ruleaza containerizat)
 - Suport pentru rulare bare-metal si virtual:
- on-premise
- virtualizate (VMware, KVM, Hyper-V)
- cloud public / privat

Funcționalități Single Sign-On:

- Autentificare centralizată pentru aplicații web și API
- Suport pentru protocoale:
 - o OAuth 2.0
 - o OpenID Connect
 - o SAML 2.0
- Federation cu:
 - o LDAP / Active Directory
 - o identity provider externi – NetIQ Identity Manager existent în infrastructura beneficiarului
- MFA / autentificare multi-factor
- politici de parolă configurabile
- sesiuni centralizate și logout global
- token management și refresh token
- suport pentru identity brokering

Cerințe de securitate:

- Patch-uri CVE furnizate prin ELS
- TLS 1.2+ obligatoriu
- criptare certificate și chei
- audit log detaliat pentru autentificări
- integrare cu SIEM – Splunk existent în infrastructura beneficiarului
- RBAC administrativ

Soluția trebuie să fie conformă cu:

- ISO 27001 (operational)
- GDPR (logare, identitate, consimțământ)
- Disponibilitate și scalabilitate:
- Suport pentru:
 - clustering
 - high availability
 - replicare baze de date
 - Load balancing extern compatibil
 - scaling vertical și orizontal
 - failover automat
- suport pentru deployment activ-activ

Integrare:

- soluția trebuie să se integreze nativ în infrastructura Red Hat Single Sign-On existentă
- soluția trebuie să fie licențiată pentru minim 32 core virtuale

Asistența producător:

- asistență 24/7 pentru 36 de luni cu timp de răspuns o oră
- acces la patch-uri critice de securitate
- bugfix-uri în regim ELS
- advisory-uri CVE
- patch-uri critice fără upgrade major

Nota: „ 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»”. Echipamentele de tip router și switch trebuie să fie produse de același producător pentru a evita problemele de interconectare.

5.7 Dezvoltare platforma de virtualizare securizata

Arhitectura Generala:

- Platforma trebuie sa fie bazata pe Kubernetes certificat CNCF.
- Implementare suportata pe infrastructura bare-metal, fara hypervisor.
- Suport pentru clustere multi-node, high-availability si disaster recovery.
- Control plane redundant
- Posibilitate de extindere orizontala fara downtime.
- Separare logica intre noduri de control si noduri de lucru.
- Suport pentru workload-uri stateless si stateful.
- Solutia trebuie sa fie licentiata pentru 6 cpu-uri.
- Sa se integreze nativ in solutia existenta bazata pe Redhat OpenShift
- Sa se integreze nativ cu Cisco ACI existent
- Sa permita backup prin intermediul IBM Spectrum Protect Plus existent

Sistem de Operare si Lifecycle:

- Sistem de operare container-optimized, hardened pentru productie.
- Actualizari atomice si rollback.
- Patch management automatizat.
- Upgrade cluster in-place, fara downtime major.
- Control al versiunilor Kubernetes si al componentelor critice.

Container Security:

- Scanare imagini container pentru vulnerabilitati.
- Politici de runtime enforcement.
- Detectie comportament anormal.
- Semnarea imaginilor container.
- Control acces bazat pe roluri (RBAC).
- Network policies native.

Compliance:

- Suport pentru ISO 27001, SOC 2, PCI DSS, HIPAA, NIS2.
- Loguri centralizate si exportabile.
- Politici de segregare a tenantilor.

Operare si monitorizare:

- Monitorizare completa pentru:
 - o cluster
 - o noduri
 - o poduri
 - o aplicatii
- Metrice Prometheus-compatible.
- Dashboard-uri Grafana-like.
- Centralizare loguri.
- Alerting configurabil.
- Tracing distribuit.

Networking:

- CNI enterprise cu suport overlay si routed.
- Load balancer intern si extern.
- Ingress controller HA.
- TLS termination.
- Service mesh optional.

CAIET DE SARCINI

- QoS si traffic shaping.
- Network segmentation.

Virtualizare si Workload Hibrid:

- Posibilitate rulare masini virtuale in cluster.
- Integrare VM + container.
- Migrare workload-uri legacy.
- Suport live migration.

Multi-Cluster si Disaster Recovery:

- Administrare centralizata multi-cluster.
- Replicare configuratii intre site-uri.
- Failover automat sau manual.
- DR orchestration.
- RPO/RTO configurabil.

Interfata si Administrare:

- Consola web enterprise.
- CLI complet.
- API REST.
- Role-based dashboards.
- Delegare administrare pe proiecte.

Servicii de asistenta producator:

- Asistenta de la producator 24/7 cu timp de raspuns 1 ora pentru 36 de luni.
- Acces la update-uri si patch-uri.

Nota: „ Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt mentionate doar pentru identificarea cu usurinta a tipului de produs si NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificatii vor fi considerate ca avand mentiunea de «sau echivalent»”. Echipamentele de tip router si switch trebuie sa fie produse de acelasi producator pentru a evita problemele de interconectare.

5.8 Echipamente 802.1x SCADA

Design Industrial
Robust

- Switch-ul trebuie să fie proiectat și construit astfel încât să fie ușor de utilizat și să nu necesite mentenanță periodică.
- Să aibă carcasă rezistentă, destinată pentru o protecție împotriva prafului, murdăriei, umidității ridicate, a câmpului electromagnetic existent în locații și a vibrațiilor.
- Racirea să fie naturală și să nu conțină componente în mișcare (de exemplu ventilatoare)
- Asistenta din partea producatorului pentru 36 de luni de tip 8X5XNBD cu timp de raspuns 30 de minute si Security Advisories, Field Notices, Priority Bugs

CAIET DE SARCINI

Conectivitate SCADA	<ul style="list-style-type: none"> Mecanism de securitate spanning Tree Protocol, clasificare de protocol SCADA, MODBUS TCP/IP, Ethernet OAM, IEEE 802.3ah, CFM (IEEE 802.1ag)
Caracteristici hardware principale	<ul style="list-style-type: none"> Minim 8 GB DRAM Minim 8 GB memorie flash
Montare	<ul style="list-style-type: none"> In rack de 19
Contacte pentru alarme	<ul style="list-style-type: none"> Două contacte pentru alarme de intrare și un contact pentru alarmă de ieșire
Porturi switch	<ul style="list-style-type: none"> 16 de Porturi (Gigabit și/sau FastEthernet, 10/100/1000 autosensing) 8 porturi sfp downlink echipate cu sfp-uri mm fastethernet si 4 porturi uplink 1/10G SFP+
Tensiuni de intrare:	<ul style="list-style-type: none"> Două surse de alimentare simultan (redundante) Tensiunea de alimentare 1 x AC/DC 85-264VAC/88-300VDC si 1 x DC 24-60V/10A
Securitate sporită	<ul style="list-style-type: none"> SSH, MAC Address Notification, Port-Security, Dynamic ARP Inspection, 802.1x cu dinamic acl, MAC Authentication, TACACS+, MACsec-128, Dinamic VLAN
Functionalitati L3	<ul style="list-style-type: none"> EIGRP conform mediu existent VRF conform mediu existent
Performante	Forwarding rate: 95.23 Mpps / Forwarding Bandwidth: 64 Gbps / IPv4 direct routes: 8192 / GRE Tunnels: 10 / Maximum SVIs: 984
Ethernet Industrial	<ul style="list-style-type: none"> Resiliență prin inele gigabit multiple Resilient Ethernet Protocol (REP) ModBus TCP SCADA Protocol Classification, Paralel Redundancy Protocol (PRP) Capacitate, scalabilitate și flexibilitate Înaltă resiliență Spanning Tree Protocol

Nota: „ Specificatiile tehnice care indica o anumita origine, sursa, productie, un procedeu special, o marca de fabrica sau de comert, un brevet de inventie, o licenta de fabricatie, sunt mentionate doar pentru identificarea cu usurinta a tipului de produs si NU au ca efect favorizarea sau eliminarea anumitor operatori economici sau a anumitor produse. Aceste specificatii vor fi considerate ca avand mentiunea de «sau echivalent»”. Echipamentele de tip router si switch trebuie sa fie produse de acelasi producator pentru a evita problemele de interconectare.

5.9 Servicii Configurare

Serviciile de livrare, configurare si integrare a echipamentelor in infrastructura existenta vor fi minimal urmatoarele:

- Toate echipamentele achizitionate se vor configura de catre Furnizor, in locatiile desemnate de catre Distribuție Energie Oltenia SA;
- Instalare si configurare solutie securitate de protectie aplicatii web si api
- Instalarea si configurare sistem de comunicatii securizate de backup pentru dispecerate
- Instalare si configurare sistem de management incidente
- Instalare si configurare solutie Load Balancer
- Instalare si configurare solutie securitate ICS
- Instalare si configurare solutie de autentificare si autorizare protaluri web
- Instalare si configurare platforma de virtualizare securizata
- Instalare si configurare echipamente 802.1x SCADA
- Integrare in solutia de monitorizare existenta Network Operating Center (NOC), bazata pe suita de produse specifice acestei solutii - IBM Tivoli
- Servicii de reconfigurare solutie de identitate utilizatori NetIQ si integrare cu solutia de autentificare si autorizare protaluri web
- Integrare pentru platforma de virtualizare securizata SCADA in SIEM-ul si SOAR existent – Splunk.
- Configurare access solutie la reseaua SCADA existenta astfel incat serverele SCADA care vor fi gazduite pe aceasta sa poate comunica cu statiile de transformare
- Configurare access pentru dipeceratele energetice din Craiova si Pitesti la solutia oferata
- Configurare solutie backup existenta (IBM Spectru Protect / Tivoli) pentru backp-ul platformei de virtualizare securizata SCADA

Distribuție Energie Oltenia SA va asigura accesul onsite la infrastructura, Furnizorul avand obligatia de a efectua analiza si obtinerea informatiilor din sistem necesare integrarii echipamentelor oferate.

Livrarea si instalarea produselor se va efectua la locatia DEO Craiova aflata la adresele de mai jos:

- Distribuție Oltenia – Craiova – jud. Dolj – str. Nicolae Titulescu nr.1

Criteriile de mai sus sunt cerinte tehnice minimale.

Service-ul in garantie se va executa la sediul beneficiarului in locatiile mentionate.

Termenul de livrare si instalare pentru toate echipamentele – maxim 90 zile de la semnarea contractului.

La finalizarea instalarii si configurarii echipamentelor si softwarelui furnizate, ofertantul va livra un document de acceptanta finala unde vor fii anexate in copie toate documentele intocmite - documentatia tehnica completa, versiune finala, revizuita si completata. Predarea de catre ofertant si acceptarea de catre Distribuție Energie Oltenia SA a documentatiei tehnice complete, reprezinta o conditie obligatorie pentru receptia sistemului.

La oferirea de produse echivalente Ofertantul va trebui sa faca dovada compatibilitatii totale a

componentelor oferite cu echipamentele existente, funcționale în infrastructura Distribuție Energie Oltenia SA.

Condiții tehnice minimale a ofertanților

Toate echipamentele care se vor instala trebuie să permită monitorizarea cu soluția existentă în prezent – Network Operating Center (NOC), bazată pe suita de produse specifice acestei soluții - IBM Tivoli;

La oferirea de produse echivalente se va face dovada compatibilității 100% cu echipamentele care funcționează în prezent în rețeaua Distribuție Energie Oltenia SA.

În vederea integrării echipamentelor achiziționate în infrastructura de comunicații existentă, exclusiv realizată folosind echipamente CISCO și soluția de monitorizare echipamente și cai de comunicații, soluție bazată pe suita de produse software IBM TIVOLI, funcțională în infrastructura autorității contractante, Ofertantul va face dovada disponibilității personalului non cheie certificat după cum urmează:

- a. Minim un consultant certificat Tivoli Monitoring V6.2 - conform mediului existent al beneficiarului.

Minim un consultant certificat Deployment Professional Tivoli Netcool/OMNIbus V7.3 - conform mediului existent al beneficiarului.

Se acceptă documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificări necesare pentru realizarea activității:

„Integrare în soluția de monitorizare existentă Network Operating Center (NOC), bazată pe suita de produse specifice acestei soluții - IBM Tivoli”

- b. Minim un consultant certificat CISCO Certified Network Professional - conform mediului existent al beneficiarului;

Se acceptă documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificări necesare pentru realizarea activității:

„Instalare și configurare echipamente 802.1x SCADA”

- c. Minim un consultant certificat CISCO Certified Network Professional Security - conform mediului existent al beneficiarului;

Se acceptă documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificări necesare pentru realizarea activității:

- „Instalare și configurare soluție Load Balancer”
- „Instalare și configurare soluție securitate de protecție aplicații web și ap”

- „Configurare access pentru dipeceratele energetice din Craiova si Pitesti la solutia ofertata”

- d. Consultanat certificat Splunk Core Certified User- conform mediului existent al beneficiarului;

Se accepta documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificari necesare pentru realizarea activitatii:

- „Integrare pentru solutia de securitate si virtualizare SCADA in SIEM-ul si SOAR existent – Splunk.’

- e. Consultanat certificat Splunk Core Certified Power User- conform mediului existent al beneficiarului;

Se accepta documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificari necesare pentru realizarea activitatii:

- „Integrare pentru solutia de securitate si virtualizare SCADA in SIEM-ul si SOAR existent – Splunk.”

- f. Minim un consultant certificat pentru solutii de securitate, Check Point Certified Security Administrator - conform mediului existent al beneficiarului;

Se accepta documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificari necesare pentru realizarea activitatii:

- ,Instalare si configurare solutie securitate ICS’

- g. Minim un consultant certificat pentru solutii de securitate, RedHat System Administrator - conform mediului existent al beneficiarului;

Se accepta documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificari necesare pentru realizarea activitatii:

- „Instalare si configurare solutie de autentificare si autorizare protaluri web”
- „Instalare si configurare platforma de virtualizare securizata”

- h. Consultanat certificat Microfocus NetIQ Identity Management certified specialist - conform mediului existent al beneficiarului;

Se accepta documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

CAIET DE SARCINI

Certificari necesare pentru realizarea activitatii:

- „Servicii de reconfigurare solutie de identitate utilizatori NetIQ si integrare cu solutia de autentificare si autorizare protaluri web”
- i. Minim un consultant certificat pentru solutii backup IBM Certified Deployment Professional - Spectrum Protect / Tivoli Storage Manager - conform mediului existent al beneficiarului;

Se accepta documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificari necesare pentru realizarea activitatii:

- „Configurare solutie backup existenta (IBM Spectru Protect / Tivoli) pentru backp-ul platformei de virtualizare securizata SCADA”
- j. Minim un consultant certificat pentru solutii management incidente Manage Engine Service Desk Plus Cerified - conform mediului existent al beneficiarului;

Se accepta documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificari necesare pentru realizarea activitatii:

- „Instalare si configurare sistem de management incidente”
-
- k. Minim un consultant certificat pentru solutii comunicatii securizate CISCO Certified Network Professional Voice - conform mediului existent al beneficiarului;

Se accepta documente echivalente emise de organisme stabilite în alte state membre ale Uniunii Europene sau cu care România are încheiate acorduri pentru recunoașterea și echivalarea certificărilor/autorizațiilor în cauză.

Certificari necesare pentru realizarea activitatii:

- „Instalarea si configurare sistem de comunicatii securizate de backup pentru dispecerate”
- l. Minim un consultant certificat pentru fiecare solutie / produs oferat;

Certificari necesare pentru realizarea activitatii de instalare a produselor oferate.

Ofertantul trebuie sa prezinte o declaratie privind personalul responsabil cu indeplinirea contractului.

La momentul ofertarii in propunerea tehnica se va prezenta modul de acces la experti/specialistii de mai sus. In propunerea tehnică va fi descris momentul în care vor interveni acești experți în implementarea viitorului contract, precum și modul în care operatorul economic ofertant și-a asigurat accesul la serviciile acestora (fie prin resurse proprii, caz în care vor fi prezentate persoanele în cauză, fie prin externalizare, situație în care se vor descrie aranjamentele contractuale realizate în

vederea obținerii serviciilor respective), iar verificarea documentelor se va face la momentul începerii prestației când vor fi prezentate certificările solicitate sau documente echivalente acestora

Un expert/specialist poate cumula mai multe certificări.

Intervenția în execuția contractului a personalului declarat (experți/specialiști) în cadrul ofertei se va efectua doar după aprobarea documentelor de către responsabilii Entității Contractante, în acest sens Contractantul se obligă să transmită aceste documente (certificările mai sus menționate) Entității Contractante înainte de începerea activităților.

Certificările cerute reprezintă dovada că Ofertantul este capabil de a asigura un standard al calității serviciilor cât și că acesta are o minimă competență profesională și performantă pentru serviciile pe care le prestează deoarece punerea în aplicare a serviciilor adiționale cerute în prezentul caiet de sarcini în capitolul “5.9. Servicii configurare” presupune accesul la temporar la sistemul informatic al beneficiarului care este operator de servicii esențiale înscris în ROSE (Registrul Operatorilor de Servicii Esențiale) care se supune legii Cyber Security 362/2018 cât și operator de date cu caracter personal care se supune directivei CE GDPR și legii 190/2018

Soluțiile software/ sisteme a căror infrastructură se dorește a fi updatată în prezentul caiet de sarcini face parte din infrastructura de servicii esențiale a Beneficiarului fiind descris în documentul de înregistrare în ROSE (Registrul Operatorilor de Servicii Esențiale) de la DNSC (Directoratul Național de Securitate Cibernetică).

La oferirea de produse echivalente Ofertantul va trebui să facă dovada compatibilității totale a componentelor oferite cu echipamentele existente, funcționale în infrastructura Distribuție Energie Oltenia SA. Infrastructura Distribuție Energie Oltenia SA cuprinde dar nu este limitată la: Switchuri LAN/WAN Cisco, Veeam Backup & Replication, VMware NSX-T, VMware vCenter 7.0, NetIQ IDM, Cisco ACI, Redhat OpenShift, Redhat SSO

6. Punere în funcțiune, testare

Contractantul trebuie să configureze toate produsele în mod corespunzător.

Contractantul va realiza și apoi toate configurările/setările necesare pentru a pune produsele în funcțiune. Punerea în funcțiune include, de asemenea, toate ajustările și setările necesare pentru a asigura configurarea corespunzătoare, în ceea ce privește performanța și calitatea, cu toate configurațiile necesare pentru o funcționare optimă.

Contractantul va efectua toate testele pentru a asigura funcționarea produsului la parametri agreeți. Contractantul rămâne responsabil pentru protejarea produselor luând toate măsurile adecvate pentru a preveni lovituri, zgârieturi și alte deteriorări, până la acceptare de către entitatea contractantă.

7. Garanție

Garanția pentru toate produsele oferite trebuie să aibă suportul producătorului datorită faptului că doar producătorul poate aduce modificări produselor sale în caz că acestea prezintă disfuncționalități sau defecte ascunse (hardware sau software). Distribuitorul nu deține proprietatea intelectuală asupra

CAIET DE SARCINI

acestora neputând presta fără suportul producătorului activitățile de dezvoltare/reparare a acestor produse ci doar de revinderea către un client final, toată această activitate (de remediere și îmbunătățire) fiind realizată în fapt de către producător

Garantia pentru:

- Dezvoltare soluție securitate de protecție aplicații web și API
- Dezvoltare sistem de comunicații securizate de backup pentru dispecerate
- Dezvoltare sistem management incidente
- Dezvoltare Soluție Load Balancer
- Dezvoltare Soluție securitate ICS
- Dezvoltare soluție de autentificare și autorizare protaluri web
- Echipamente 802.1x SCADA

trebuie să aibă următoarele facilități:

Garantia hardware a tuturor modulelor din compunerea sistemului oferit și livrat va fi de minim 36 luni; Garantă hardware va fi asigurată cu un SLA (Service Level Agreement) de 8x5xNBD (8 ore pe zi, 5 zile pe săptămână, cel mai târziu a doua zi lucrătoare - Next Business Day), care să garanteze diagnosticarea componentei sau modulului defect și înlocuirea acestuia în maxim 3 zile lucrătoare, fără alte costuri suplimentare pentru beneficiar;

Garantia software-ului aferent modulelor ce intră în compunerea sistemului va fi cea indicată de producătorul acestuia. Se va asigura aducerea la zi gratuită a versiunilor software-ului specific fiecărui modul din compunerea sistemului (servere, stocare, salvare date, comunicație etc.) pe o perioadă de minim 36 de luni, corespunzătoare garanției hardware;

Toate componentele trebuie să fie în conformitate cu standardele impuse prin Directiva UE 2015/863 (RoHS 3).

Suportul software va fi de minim 36 luni. Se va asigura acces la centrul de suport al producătorului, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software (sistem de operare, firmware etc.) ori de câte ori este necesar. Se va asigura posibilitatea de a semnaliza și a cere rezolvarea problemelor de nefuncționare datorate problemelor software, prin escaladarea acestora la centrul de suport al ofertantului sau al producătorului;

Se vor preciza part-number-ul (-ele) care asigură condițiile de garanție hardware și suport software mai sus menționate.

Garantia pentru produsele de la Dezvoltare platforma de virtualizare securizată trebuie să aibă următoarele facilități:

Suportul software va fi de minim 36 luni. Se va asigura acces la centrul de suport al producătorului, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora în funcție de severitate. De asemenea se va asigura dreptul de a face update-uri și upgrade-uri la toate componentele software (sistem de operare, firmware etc.) ori de câte ori este necesar. Se va asigura posibilitatea de a semnaliza și a cere rezolvarea problemelor de nefuncționare datorate problemelor software, prin escaladarea acestora la centrul de suport al ofertantului sau al producătorului;

Se vor preciza part-number-ul (-ele) care asigură condițiile de garanție hardware și suport software

mai sus mentionate.

Responsabilitățile furnizorului în ceea ce privește garanția acordată sunt:

Produsele livrate upgrdate trebuie să fie înregistrate de către Furnizor la producător. În cazul în care un produs nu este înregistrat la producător, part-number-ul și seria-number-ul nu apar pe site-ul producătorului cu garanție hardware și suport software, Entitatea Contractantă va returna produsul, fără a plăti contravaloarea acestuia, Furnizorul având obligația de a înlocui produsul cu unul care este înregistrat la producător. Înscriserea produselor pe site-ul producătorului asigură cel puțin downloadarea ultimelor versiuni de software și firmware, incluzând capacitatea beneficiarului de a deschide cazuri de suport tehnic direct la producător prin siteul web al producătorului și telefon.

- diagnosticarea componentei hardware sau modului defect și înlocuirea acestuia în maxim 3 zile lucrătoare.
- actualizarea/aducerea la zi a versiunilor software-ului specific fiecărui modul din compunerea sistemului (servere, stocare, salvare date, comunicare etc.).
- update-uri și upgrade-uri la toate componentele software (sistem de operare, firmware etc.) ori de câte ori este necesar.
- suport tehnic prin site-ul web și telefon, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora, pentru probleme legate de aplicare de patchuri, disfuncționalități minore care nu au impact în funcționarea produsului, upgrade de firmware sau software la cerere.

Responsabilitățile producătorului în ceea ce privește garanția sunt:

- asigură acces pentru downloadarea ultimelor versiuni de software și firmware.
- suport tehnic prin siteul web și telefon, cu posibilitatea raportării problemelor aparute în funcționare și solicitarea rezolvării acestora, pentru probleme legate de disfuncționalități în software sau firmware care presupun dezvoltarea de patchuri de Securitate sau dezvoltarea unei noi versiuni de software sau firmware.

În cazul apariției unor neconformități ale produselor hardware și software, având în vedere faptul că producătorul nu este parte în contractul de achiziție încheiat, entitatea contractantă se va adresa producătorului în baza garanției oferite de producător care trebuie să fie formalizată printr-un certificat/document de garanție (care poate fi fizic sau electronic) în care să fie specificat în mod clar că beneficiarul garanției oferite de producător este utilizatorul final al produsului. Furnizorul va prezenta certificatul/documentul de garanție la livrarea produselor hardware și software.

8. Livrare, ambalare, etichetare, transport și asigurare pe durata transportului

Termenul de livrare este cel menționat pentru fiecare produs în parte. Un produs este considerat livrat când toate activitățile în cadrul contractului au fost realizate și produsul/echipamentul este instalat, funcționează la parametrii agreeți și este acceptat de entitatea contractantă.

Fiecare produs va fi însoțit de toate subansamblele/partile componente necesare punerii și mentinerii în funcțiune.

Contractantul va ambala și eticheta produsele furnizate astfel încât să prevină orice daună sau deteriorare în timpul transportului acestora către destinația stabilită.

Dacă este cazul, ambalajul trebuie prevăzut astfel încât să reziste, fără limitare, manipularii accidentale, expunerii la temperaturi extreme, șarii și precipitațiilor din timpul transportului și depozitării în locuri deschise. În stabilirea mărimumi și greutății ambalajului Contractantul va lua în considerare, acolo unde este cazul, distanța față de destinația finală a produselor furnizate și eventuale absența a facilităților de manipulare la punctele de tranzitare.

CAIET DE SARCINI

Toate costurile aferente transportului, inclusiv asigurarea împotriva pierderii sau deteriorării intervenite pe parcursul transportului și cauzate de orice factor extern vor fi incluse în prețul ofertei.

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

8.1 DOCUMENTATII CE TREBUIE FURNIZATE ENTITATII CONTRACTANTE ÎN LEGATURA CU PRODUSUL

Documentatiile pe care Contractantul trebuie să le livreze Entității Contractante sunt menționate în specificația tehnică atasată la caietul de sarcini.

La livrare produsele vor fi însoțite de următoarele documente:

- certificat de conformitate al produsului;
- certificat de calitate;
- certificat de garanție;
- instrucțiuni de întreținere și exploatare în limba română sau engleză.

La finalizarea instalării și configurării echipamentelor și softwareului furnizate, furnizorul va livra un document de acceptanță finală unde vor fi anexate în copie toate documentele întocmite - documentația tehnică completă, versiune finală, revizuită și completată. Predarea de către furnizor și acceptarea de către Distribuție Energie Oltenia SA a documentației tehnice complete, reprezintă o condiție obligatorie pentru recepția sistemului.

La oferirea de produse echivalente Ofertantul va trebui să facă dovada compatibilității totale a componentelor oferite cu echipamentele existente, funcționale în infrastructura Distribuție Energie Oltenia SA.

8.2 RECEPȚIA PRODUSELOR

Recepția produselor se va efectua pe baza de proces verbal semnat de Contractant și entitatea contractantă. Recepția produselor se va realiza în mai multe etape, în funcție de progresul contractului, respectiv:

- a) recepția cantitativă se va realiza în maxim 5 zile după livrarea produselor în cantitatea solicitată la locația indicată de entitatea contractantă
- b) recepția calitativă se va realiza în maxim 5 zile după configurarea și integrarea produselor. Furnizorul are obligația de a remedia defectele, identificate de către Entitate prin procesul verbal de recepție calitativă, în termen de maxim 30 de zile de la semnarea procesului verbal de recepție calitativă.

Procesul verbal de recepție calitativă va include unul din următoarele rezultate:

- a) acceptat;
- b) acceptat cu observații minore;
- c) acceptat cu rezerve;
- d) refuzat.

8.3 MANAGEMENTUL/GESTIONAREA CONTRACTULUI SI ACTIVITATI DE RAPORTARE ÎN CADRUL CONTRACTULUI

Entitatea contractanta va raspunde de managementul contractului si de sarcinile specifice, va urmări indeplinirea contractului pe toata perioada de implementare a acestuia, asigurand toate activitatile care decurg din drepturile si obligatiile stabilite prin acesta. Modul de comunicare in implementare se face prin mail si intalniri on-site si online. Mecanismul de monitorizare a bunurilor livrate de furnizor se va face pe baza proceselor verbale de receptive incheiate intre entitatea contractanta si furnizor.

Furnizorul este responsabil pentru indeplinirea urmatoarelor atributii:

- Indeplinirea obligatiilor care decurg contract in conformitate cu cerintele legislatiei aplicabile si a prevederilor prezentei documentatii de atribuire

Colaborarea cu personalul Entitatii contractante alocat derularii contractului (monitorizarea indeplinirii activitatilor si coordonarea activitatilor):

Entitatea contractanta este responsabila pentru indeplinirea urmatoarelor atributii:

- Punerea la dispozitia furnizorului a tuturor informatiilor necesare pentru realizarea contractului
- Verificarea cantitativa si calitativa a produselor pentru a stabili conformitatea acestora cu cerintele prezentei documentatii de atribuire

Efectuarea platilor aferente produselor livrate de catre Furnizor, in termenele convenite, in baza procesului verbal de receptie aprobat fara obiectiuni de catre Entitatea contractanta.

Tipul de risc	Entitate Responsabila	Risc	Modalitati de gestionare
De natura contractuala	Beneficiar	Neindeplinirea obligatiilor asumate	Monitorizarea contractului din punct de vedere al indeplinirii obligatiilor contractuale. Aplicarea si respectarea clauzelor contractuale.
De natura tehnica	Furnizor	Livrarea unor echipamente ne-conforme	Respectarea specificatiilor tehnice, livrarea de produse conform ofertei tehnice declarate si respingerea de catre entitatea contractanta a produselor neconforme.
De natura financiara	Beneficiar	Neplata la termen a facturilor	Monitorizarea permanenta a latilor, cu respectarea termenelor de plata si evitarea intarzierilor la plata.

CAIET DE SARCINI

De timp	Furnizor	Intarzierea in livrarea Produselor la termenele solicitate	Entitatea contractanta transmite comenzile de aprovizionare in timp util. Furnizorul livreaza produsele in termenul contractual astfel incat sa nu se genereze intarzieri in desfasurarea activitatilor entitatii Contractante.
---------	----------	--	--

Se vor respecta toate cerintele impuse in caietul de sarcini si specificatiile tehnice;

9. Cerințe privind Practicile Etice, Conduita în Afaceri și Conformitatea:

Activitatea DEO se bazează pe un set de valori etice și linii directoare cuprinse în documentele denumite: “Codul de Etică”, “Codul de Conduită în afaceri”, „Manualul de Conformitate” in baza caruia a fost intocmit „Codul de Conduită pentru Furnizori”. Aceste documente reflectă angajamentul Părților de a respecta toate prevederile legale aplicabile în domeniul lor de activitate, emise la nivel național, european sau internațional. Documentele pot fi consultate pe site-ul www.distributieoltenia.ro, in subsecțiunea “Etica si Integritate”.

În cazul unei modificări a cadrului legal și/sau de reglementare, precum și în cazul pronunțării unei hotărâri judecătorești, Părțile se angajează să adopte imediat ajustările necesare ale clauzelor contractuale în vederea remedierii situației.

Furnizorul se angajează să respecte și să solicite directorilor, angajaților și afiliaților lor să respecte la rândul lor prevederile Codului de conduită al Furnizorului, precum și legislația în vigoare (denumite în continuare „Regulile”) și declară că:

1. fiecare dintre persoanele prevăzute în prezentul paragraf și care va fi implicat în mod direct sau indirect, în orice mod, în executarea Contractului, precum și orice măsuri adoptate, directe sau indirecte, de natură tehnică, financiară și operațională necesare pentru executarea Contractului, respectă Regulile;
2. respecta sancțiunile economice internaționale care restricționează vânzarea bunurilor și a serviciilor către anumite țări sub embargo sau către persoane vizate de astfel de sancțiuni.

Pe toată durata contractului Furnizorul se obligă să respecte Regulile și

1. în orice moment al executării Contractului va fi în măsură să furnizeze la solicitarea celeilalte Părți toate elementele solicitate pentru a se verifica respectarea Regulilor și
2. va informa de îndată cealaltă Parte atunci când au cunoștința de nerespectarea în orice mod a Regulilor de către o persoană precizată la paragraful (3), precum și măsurile corective adoptate pentru a asigura respectarea acestora.

Responsabilitatea Partenerului/Furnizorului este de a se asigura că angajații săi au fost informați cu privire la prevederile prezentei clauze și au implementat reguli adecvate pentru a se asigura de conformarea cu aceste cerințe. DEO solicită Partenerului/Furnizorului și subcontractorilor Partenerului/Furnizorului să adere la standarde identice cu ale sale, prevăzute în “Codul de Etică”, “Codul de

CAIET DE SARCINI

Conduită în afaceri”, „Manualul de Conformitate”. În particular, Partenerul/ Furnizorul se obligă să se conformeze și să facă astfel încât subcontractorii săi și orice persoană aflată sub controlul său să se conformeze acestei clauze și standardelor în vigoare.

Partenerul/ Furnizorul va defini și va implementa politici efective corespunzătoare pentru a asigura conformarea și o va verifica în mod regulat. Partenerul/ Furnizorul va informa DEO, la cerere, despre măsurile adoptate pentru a asigura conformarea.

Nerespectarea clauzei de conduita a Furnizorului va fi considerată ca fiind o încălcare grava a Contractului, fapt care poate duce la încetarea raporturilor contractuale.

10. Cerințe privind prelucrarea DCP

Ofertantul declarat câștigător are obligația să furnizeze răspunsuri care reflectă în mod exact situația sa, la toate întrebările cuprinse în Chestionarul de conformitate GDPR (anexat prezentului Caiet de Sarcini); în termen de 5 zile lucratoare de la data la care este declarat castigator. Omisiunea furnizării de răspunsuri complete sau furnizarea unor răspunsuri inexacte va da dreptul DEO să înceteze raporturile contractuale cu ofertantul declarat câștigător imediat ce va descoperi aceste inexactități.

Informațiile furnizate de ofertant prin completarea Chestionarului de conformitate GDPR vor fi utilizate de beneficiar numai pentru evaluarea gradului de conformitate GDPR al ofertantului câștigător și nu în scopul evaluării ofertelor concurente.

11. Cerințe SSM, aplicabile în perioada de derulare a contractului

În termen de 10 zile de la semnarea contractului (documentele solicitate se semnează la nivel de DEO) va semna și va transmite achizitorului următoarele documente:

- ✓ **Metodologie de lucru privind modalitatea de derulare a contractului;**
- ✓ **Anexa 2: Convenția de lucrări pentru serviciul prestat**

11.1 Cerințe SSM privind obligațiile contractanților

La executarea lucrărilor se vor respecta prevederile următoarelor acte normative:

- Convenția de Lucrări încheiată între Contractant ca executant de lucrări și DEO
- OUG 195/2002 privitoare la circulația pe drumurile publice (Codul Rutier) (reactualizată);
- Legea securității și sănătății în muncă actualizată (nr. 319/2006);
- HG nr. 971/2006 privind cerințele minime pentru semnalizarea de securitate și/sau de sănătate la locul de muncă;
- HG nr. 1028/2006 privind cerințele minime de securitate și sănătate în muncă referitoare la utilizarea echipamentelor cu ecran de vizualizare;
- HG nr. 1048/2006 privind cerințele minime de securitate și sănătate pentru utilizarea de către lucrători a echipamentelor individuale de protecție la locul de muncă;
- HG nr. 1425/2006 pentru aprobarea Normelor metodologice de aplicare a prevederilor Legii securității și sănătății în muncă, nr. 319/2006 completată și modificată
- HG nr. 355/2007 privind supravegherea sănătății lucrătorilor.

Este necesar ca la aplicarea normelor specifice să se țină seama și de prescripțiile naționale de securitate și sănătate a muncii, obligatorii ca documente complementare:

11.2 Conditii privind sanatatea si securitatea muncii la executarea lucrarilor/ prestarea serviciilor**SSM. 1. Domeniu de aplicare**

Prezentele Conditii privind sanatatea si securitatea muncii ("conditiile SSM") guverneaza obligatiile partilor in legatura cu problemele legate de sanatate si securitate in munca ale Contractului (astfel cum sunt definite mai jos)

Preambul

- 1.1** Prezentul document ofera Ofertantilor informatii esentiale privind aspectele semnificative ale sanatatii si securitatii in munca pe care Contractantul si subcontractantii le vor aborda in timpul activitatii in numele Distributie Energie Oltenia.
- 1.2** Contractantul si subcontractantii vor utiliza aceste informatii pentru a elabora o documentatie corespunzatoare si suficienta privind SSM, identificand masurile de SSM care trebuie implementate in timpul desfasurarii activitatilor contractuale definind costurile aferente, promovand cele mai bune practici in managementul SSM. Fiecare cerinta inclusa in acest document trebuie implementata atunci cand exista un pericol specific.
- 1.3** Informatiile raportate in prezentul document vor fi considerate conditii contractuale.
- 1.4** Pentru DEO, protectia sanatatii, securitatii, integritatii fizice si psihologice a persoanelor nu este doar o obligatie legala, ci si o responsabilitate morala fata de angajatii si contractantii sai.
- 1.5 In cadrul DEO, nu se pot efectua lucrari in detrimentul SSM. Din acest motiv orice situatie de risc sau comportament nesigur va determina suspendarea lucrarilor pana la reimplementarea conditiilor de securitate.**

DEO se implica putemic si in mod constant in promovarea consolidarea unei culturi a sanatatii si securitatii muncii, promovand acordarea unei atentii sporite situatiilor de risc si constientizarea acestora, incurajand adoptarea unor comportamente responsabile din partea celor care lucreaza cu si pentru DEO

SSM. 2. OBLIGATII SSM GENERALE

2.1. Contractantul se angajeaza sa isi indeplineasca obligatiile care decurg din Contract astfel sa asigure zone de lucru sigure si sanatoase atat pentru personalul propriu, personalul DEO implicat cat si pentru terti In acest scop, Contractantul se angajeaza:

- a) sa respecte legislatia** aplicabila in domeniul sanatatii si securitatii in munca
- b) sa respecte toate instructiunile proprii, specifice , tehnice de securitatea muncii** precum si alte documente care fac referire la respectarea sanatatii si securitatii in munca
- c) sa respecte bunele practici din domeniu**, luand in considerare principiile stabilite in Politica adoptata de DEO si obiectivele generale
- d) sa coopereze cu DEO si cu alti contractanti** in vederea imbunatatii continue a sanatatii si securitatii astfel incat prin masurile adoptate sa previna sau sa diminueze riscurile de accidentare
- e) sa furnizeze DEO informatii imediate cu privire la orice problema legata de SSM** care ar putea avea efecte grave asupra personalului propriu sau asupra personalului DEO si poate afecta, periclita, intarzia activitatile Contractului

2.2. Fara a aduce atingere nivelului de implicare al DEO in probleme de sanatate si Securitate in munca Contractantul ramane responsabil pentru orice dauna asupra sanatatii si securitatii provocate de acesta, de personalul sau sau din vina subcontractantilor.

Contractantului ii revine raspunderea integrala pentru :

- respectarea cerintelor legale in vigoare, precum, a instructiunilor de securitate si sanatate in munca precum si conventia de lucrari incheiata intre parti;

CAIET DE SARCINI

- asigurarea calitatatii lucrarilor si respectarii cerintelor din fisele tehnologice precum si a tuturor reglementarilor in vigoare care stau la baza executiei acestora;

Contractantul va respecta obligatoriu si urmatoarele cerinte minime de SSM

- Contractantul isi va putea indeplini obligatiile asumate, numai dupa incheierea Conventiilor de lucrari (impreuna cu anexele care fac parte integranta din conventie),
- Personalul Contractantului va fi echipat corespunzator riscurilor la care este expus
- Personalul Contractantului va fi instruit periodic conform legislatiei in vigoare
- Echipamentele de munca utilizate la lucrari de catre personalul delegat trebuie sa fie certificate conform prevederilor legale;
- Personalul delegat nu are voie sa paraseasca zona de lucru
- **Contractantul va suporta contravaloarea sanctiunilor (amenzi, daune, despagubiri etc.) suportate de Achizitor ca urmare a incalcarii de catre Contractant a obligatiilor legale ce ii revin in materie de SSM, prin retinere din sumele pe care i le datoreaza Achizitorul.**

In cazul in care, pe durata inspectiilor si a controalelor desfasurate in faza de executie a lucrarilor, sunt depistate incalcari grave sau foarte grave in materie de securitatea muncii (Lista incalcarilor grave si foarte grave in materie de SSM) de catre Contractant sau de catre angajatii acestuia succesiv, in raport cu gravitatea incalcarii comise, Achizitorul va evalua care din urmatoarele actiuni vor fi luate impotriva contractantului: **aplicarea penalitatilor, suspendarea lucrarilor, excluderea de la executarea lucrarilor a formatiei de lucru pe teritoriul DEO (daca se constata incalcarea de maxim 3 ori succesiv) rezilierea contractului pentru incalcarea legislatiei in materie de sanatate si securitatea muncii.**

Penalitatiile aplicate vor fi urmatoarele: 10000 lei pentru incalcari grave (G) si 20000 lei pentru incalcari foarte grave (FG).

La solicitarea contractorului, DEO poate decide să nu aplice penalitățile aferente abaterilor constatate, incadrate conform listei de mai jos, în situația în care Contractantul se angajeaza sa achizitioneze pentru echipele proprii echipamente individuale de protectie, intr-un termen convenit impreuna cu Achizitorul. In situatia in care, in termenul convenit, Contractantul nu face dovada că echipamentele corespunzătoare au fost achiziționate și date spre utilizare echipelor acestuia, Achizitorul aplica penalitatiile aferente abaterilor constatate.

Penalitatiile aplicate nu vor depasi valoarea contractului.

**LISTA (NEEXHAUSTIVA) A INCALCARILOR GRAVE (G) SI FOARTE GRAVE (FG)
IN MATERIE DE SECURITATE SI SANATATE IN MUNCA**

Prevederi cu caracter general	Neefectuarea comunicarii catre DEO imediat a accidentelor de munca mortale sau grave (cu prim prognostic mai mare de 30 de zile sau cu prognostic rezervat) sau, indiferent de prognostic, a accidentelor de natura electrica sau prin cadere de la inaltime	FG
	Neefectuarea comunicarii catre DEO (in cel mult 24 h de la eveniment) a accidentelor usoare in munca (cu prim prognostic de la 1 la 30 de zile)	G
	Utilizare personal neautorizat	FG
	Utilizare neautorizata de aparaturi, echipamente si sisteme de securitate	FG
	Nedelimitarea materiala a zonelor de lucru	FG
	Adoptarea incompleta/eronata a indicatoarelor de securitate in zona de lucru	G
	Depistarea consumului de alcool sau substante stupefiante la locul de munca	FG
	Nerespectarea indicatoarelor privind siguranta	G

CAIET DE SARCINI

	Amplasarea neadecvata a materialelor in zona de lucru	G
	Instruirea și supravegherea membrilor formației de lucru	FG
	Intrarea in zona de lucru fara instiintarea prealabila a DEO	FG
	Documente SSM intocmite neconform sau lipsa de la lucrare	G
	Echipamente de lucru la inaltime neconforme (de ex: scari deteriorate, fara sistem de asigurare pe stalp si prevazute cu opritor de cadere)	FG

NOTA: Incalcarea repetata este considerata un element agravant al incalcarii si reclasifica incalcarea grava intr-una foarte grava

SSM. 3. OBLIGATII SSM SPECIFICE

3.1. Contractantul va folosi personalul angajat in conformitate cu legislatia aplicabila

3.2. Contractantul va respecta toate instructiunile de sanatate si securitate in pentru fiecare punct/zona de lucru, inclusiv planurile de urgenta in acest scop

Contractantul trebuie sa se asigure ca pentru zonele de lucru aflate sub controlul sau, a stabilit si a comunicat instructiuni adecvate in materie de sanatate si securitate in munca tuturor persoanelor prezente in orice moment in zona de lucru si a instituit proceduri adecvate de monitorizare de respectare a acestor instructiuni de catre toate aceste persoane

3.3. In timpul deplasarii intre punctele de lucru, personalul Contractantului trebuie sa respecte intotdeauna codul rutier aplicabil

3.4. Se interzice in toate zonele de lucru:

- a) sa detina sau sa utilizeze arme de foc sau munitie pentru arme de foc
- b) sa consume sau sa se afle sub influenta alcoolului, narcoticelor sau substantelor psihotrope ilegale,

SSM. 4. CONSTIENTIZARE SI COORDONARE SSM
4.1. Instruirea la inceperea activitatii

Inainte de inceperea activitatilor contractuale DEO va instrui participantii la lucrare cu documentele lucrarii (conventie de lucrari) si riscurile aferente acestora conform deciziei de instruire DEO in conformitate cu legislatia in vigoare

4.2. Verificari inainte de inceperea lucrarilor

Imediat inainte de inceperea fiecarei lucrari Contractantul, prin seful de lucrare, va efectua verificari privind securitatea zonei de lucru, se va asigura ca personalul din subordinea sa sau cel al subcontractantilor a inteles riscurile care pot sa apara, descrie echipamentul utilizat si comportamentul pe care membrii formatiei de lucru trebuie sa-l adopte pentru a preveni incidentele

Aceste verificari trebuiesc repetate ori de cate ori se produce o schimbare a conditiilor de lucru sau un nou lucrator este introdus la lucrare.

SSM. 5 . RAPORTAREA ACCIDENTELOR /INCIDENTELOR/ SITUATIILOR PERICULOASE

Contractantul va comunica imediat catre DEO orice eveniment/ incident cu potential ridicat de accident sau accident de munca in care a fost implicat personalul propriu in timpul executarii lucrarilor prin notificare scrisa care sa contina o descriere detaliata a evenimentului, toate informatiile preliminare disponibile In cazul in care DEO desemneaza un grup de analiza pentru a investiga cauzele unui eveniment/incident periculos sau accident de munca Contractantul trebuie sa coopereze pe deplin pentru orice informatie care

poate fi solicitata.

SSM. 6. MONITORIZARE

DEO are dreptul sa efectueze inspectii sau audituri pentru a controla respectarea obligatiilor SSM. Daca in timpul inspectiilor se constata neconformitati DEO va notifica Contractantul in acest sens. In 3 zile Contractantul va furniza clarificari privind motivele care au generat neconformitatea , precum si masurile de remediere generate.

SSM. 7. NECONFORMITATI SSM

Contractantul trebuie sa urmareasca toate neconformitatile detectate in timpul inspectiilor (de catre personalul SSM propriu sau personalul DEO) si masurile corective luate.

12. ANEXE

- Chestionarul de conformitate GDPR;
- Notificare de confidentialitate specifica achizitiei disponibila aici:
<https://www.distributieoltenia.ro/ro/protectia-datelor-personale/note-de-informare-privind-prelucrarea-datelor-personale.html>
- **Anexa 1: Conventia de lucrari pentru serviciul prestat**

13. Reglementari aplicabile care trebuie respectate

- Sunt cele mentionate in specificatiile tehnice inclusiv normativa europeana de comercializare a produselor prin inscripționare cu marcajul CE.
- GDPR

Anexa 1: Convenția de lucrări pentru serviciul prestat**CONVENȚIE DE LUCRARI**
(Anexa la contractul nr.....)**CAP. I ENTITĂȚILE SEMNATARE:**

(1) **1. DISTRIBUȚIE ENERGIE OLTENIA SA** în calitate de beneficiar, reprezentată prin _____ denumită în continuare **“Beneficiar”**

și

(2) **1.2. S.C. S.A./ S.R.L.,**..... societate legal constituită și funcționând în conformitate cu legile române, cu sediul social în _____, cod unic de înregistrare fiscală CUI _____, nr. Registrul Comerțului _____, reprezentată legal prin _____, (**„Prestatorul”**); denumită în continuare **„Prestator”**

CAP. II OBIECTUL ȘI SCOPUL CONVENȚIEI

2.1. Convenția stabilește obligațiile și răspunderile ce intervin în relațiile dintre părți, privind securitatea și sănătatea în muncă, protecția mediului, apararea împotriva incendiilor, protecția civilă și în vederea evitării accidentelor, îmbolnăvirilor profesionale, poluării mediului și prevenirea incendiilor, precum și luarea de măsuri pentru înlăturarea consecințelor acestora în conformitate cu prevederile legale în vigoare.

CAP. III DENUMIREA LUCRĂRII CONTRACTATE / SERVICIULUI CONTRACTAT

POLITICA STOP ACTIVITATE privind consolidarea culturii de sănătate și siguranță

În cadrul Distribuție Oltenia ne angajăm permanent să promovăm și să consolidăm cultura de sănătate și siguranță a tuturor persoanelor implicate în activitatea noastră.

Pentru noi, oamenii sunt cea mai prețioasă resursă și este responsabilitatea noastră să protejăm siguranța tuturor angajaților și partenerilor noștri. Această responsabilitate înseamnă conștientizarea riscurilor și încurajarea unui comportament responsabil pentru a ne asigura că toate activitățile se desfășoară cu responsabilitate, implicare și fără accidente.

Considerăm că nu există lucrare suficient de urgentă încât să nu putem dedica tot timpul necesar realizării acesteia în siguranță.

Prin Politica STOP ACTIVITATE, toți angajații, partenerii și contractorii Distribuție Oltenia sunt împuterniciți să oprească activitățile de lucru considerate a fi un pericol iminent, cele în care sunt identificate condiții sau comportamente care ar putea provoca moartea unor persoane sau vătămări grave.

Reluarea activității se va face întotdeauna numai după îndepărtarea pericolului și asigurarea unui loc de muncă sigur.

Prin urmare, vă solicităm fiecăruia dintre dumneavoastră să acționați rapid și să opriți orice activitate care prezintă sau poate prezenta un risc pentru sănătatea și siguranța dumneavoastră sau a altora.

De asemenea, vă solicităm să raportați imediat superiorului dumneavoastră direct sau Direcției Sănătate & Securitate în Muncă orice comportament riscant și orice acțiune, omisiune sau situație care ar putea provoca

un accident sau daune aduse mediului.

Ordinul de oprire a lucrărilor trebuie pus în aplicare fără teama de consecințe.

Nu va fi atribuită nicio vină sau răspundere angajaților, partenerilor sau contractanților care raportează cu bună credință o situație riscantă sau care opresc lucrul, chiar dacă o astfel de acțiune se dovedește a fi ulterior inutilă.

Sănătatea și siguranța fiecăruia dintre noi reprezintă angajamentul nostru zilnic și prioritatea principală, mai presus de toate celelalte cerințe.

CAP. IV RESPONSABILITĂȚI PRIVIND REALIZAREA MASURILOR DE SECURITATE ȘI SANATATE ÎN MUNCA, PROTECȚIA MEDIULUI, APARAREA ÎMPOTRIVA INCENDIILOR ȘI PROTECȚIA CIVILĂ

A. PREVEDERI DE SANATATE ȘI SECURITATE ÎN MUNCA (SSM)

A1. Obligațiile principale ale Beneficiarului:

- Beneficiarul asigură informarea lucrătorilor Prestatorului, pentru îndeplinirea activităților pe care aceștia trebuie să le desfășoare în conformitate cu obiectul Contractului de prestări servicii încheiat între părți, și cu prevederile legale în vigoare;
- Beneficiarul întocmește fișa de instruire colectivă în conformitate cu prevederile Legii 319/ 2006 și a Normelor metodologice de aplicare a acestei legi, H.G. 1425/ 2006 completată cu H.G. 955 / 2010, HG 1242/ 2011 și H.G. 767 / 2016
- Să asigure la sediul/sediile sale secundare, condițiile de lucru adecvate bunei desfășurări a activității de către lucrătorii Prestatorului;
- Să doteze și să amenajeze corespunzător locurile/spațiile unde salariații proprii ai Prestatorului își realizează activitatea, în conformitate cu prevederile legislației de securitate și sănătate în muncă;
- Să aplice măsurile de oprire a activității atunci când situația o impune pentru neîndeplinirea cerințelor legale din punct de vedere al sănătății și securității în muncă
- Să permită necondiționat accesul serviciilor de urgență și al persoanelor care acordă ajutor conform instrucțiunilor specifice, fiecare pentru personalul propriu;
- Controlează modul de aplicare a prevederilor legale de SSM.

A2. Obligațiile principale ale Prestatorului:

- Prestatorul, prin salariații săi / salariații care lucrează în numele său, prestează serviciile în condițiile, la standardele de calitate, la termenele și conform programului stabilit de către Beneficiar, și potrivit dispozițiilor legale în materie;
- Având în vedere faptul că în activitatea desfășurată conform prevederilor contractului, prestatorul(executantul) lucrează independent cu personal și mijloace tehnice proprii, poartă întreaga responsabilitate asupra respectării legislației de securitate a muncii pentru întreaga activitate prestată;
- Prestatorul(executantul) poartă întreaga răspundere în cazul producerii accidentelor de muncă, evenimentelor și incidentelor periculoase, îmbolnăvirilor profesionale generate sau produse de echipamentele tehnice (utilaje, instalații etc.) și de muncă, procedeele tehnologice utilizate, sau de către lucrătorii săi și cei aparținând societăților care desfășoară activități pentru antreprenorul general (subcontractanți), în conformitate cu prevederile Legii securității și sănătății în muncă nr. 319/2006 și a Normelor metodologice de aplicare a Legii nr. 319/2006 aprobate prin H.G. nr. 1425/2006, precum și orice modificare legislativă apărută pe timpul desfășurării contractelor;
- Prestatorul efectuează evaluarea sau reevaluarea (după caz) a riscurilor de accidentare și/sau îmbolnăviri profesionale pentru locurile în care își desfășoară activitatea salariații săi și pentru propriile activități conform cerințelor Legii nr. 319/2006, cu evaluator atestat. Rezultatul evaluării este adus la cunoștința angajaților Prestatorului;
- Prestatorul întocmește planul de prevenire și protecție bazat pe evaluarea riscurilor de accidentare și îmbolnăvire profesională;

CAIET DE SARCINI

- Prestatorul instruieste si intocmeste angajatilor sai proprii fisa de instruire individuala privind securitatea si sanatatea in munca si efectueaza instruirea introductiv generala precum si orice alte instruiiri cu privire la salariatii sai, conform prevederilor legale;
- Prestatorul isi instruieste proprii lucratori pentru activitatile desfasurate, in conformitate cu prevederile art. 74 – 100 din Normele Metodologice actualizate de aplicare a prevederilor Legii nr. 319/2006 si instruirea la locul de munca si periodic. Aceste instruiiri se efectueaza cu consemnarea in fisele individuale de instruire in domeniul SSM si sunt pastrate la Prestator. Instruirea se face cu riscurile pentru securitatea si sănătatea lor, precum si măsurile si activitățile de prevenire si protecție valabile in incinta si la locul de munca aflate in zona de lucru a Prestatorului, pe care Beneficiarul il pune la dispozitia Prestatorului la solicitarea acestuia;
- Deoarece Prestatorul (executantul) desfasoara o activitate independenta cu personal si mijloace tehnice proprii, Prestatorul poarta intreaga raspundere legala privind modul de instruire a personalului propriu in toate fazele, modul de consemnare a instruirii, etc.
- Prestatorul isi doteaza proprii lucratori cu echipament individual de protectie, specific activitatii prestate in functie de riscurile de accidentare evaluate, existente la locurile de de munca unde lucratorii/salariatii proprii ai Prestatorului isi desfasoara activitatea;
- Prestatorul efectueaza controlul medical al salariatilor sai (si la angajare si periodic) prin servicii de medicina muncii, conform prevederilor legale;
- Prestatorul informeaza si pune la dispozitia Beneficiarului toate datele necesare acestuia din urma cu privire la salariatii sai in ceea ce priveste securitatea si sanatatea in munca, medicina muncii, etc;
- Orice eveniment produs in activitati organizate de Prestator, este comunicat de indata de catre acesta , Beneficiarului, Inspectoratului Teritorial de Munca si Casei judetene de Pensii si, dupa caz, Parchetului de pe lângă Judecătoria locala;
- Cercetarea accidentelor care au antrenat incapacitate temporara de munca si care au ca victime lucratori ai Prestatorului se face de catre acesta;
- Cercetarea accidentelor urmate de invaliditate evidenta sau deces se face sub supravegherea ITM;
- Cercetarea altor tipuri de evenimente se face conform normelor in vigoare.

A3. Personalul delegat:

- Conducerea formatiei de lucru apartine sefului acesteia, sub aspectul distribuirii sarcinilor si efectuarea instruirii pentru prevenirea accidentelor;
- Pe durata realizarii activitatilor seful de lucrare trebuie sa ia masuri pentru evitarea accidentarii sale sau a membrilor formatiei cu care realizeaza operatiile pregatitoare, respectand reglementarile proprii;
- In timpul executarii lucrarii, seful de lucrare trebuie sa se afle in permanenta in zona de lucru asigurand controlul activitatii formatiei de lucru, supravegherea membrilor acesteia sau participarea la lucrarea incredintata;
- Personalul delegat executa lucrari folosind personal:
 - instruit periodic, conform legislatiei de securitatea muncii in vigoare, tinand seama de conditiile de lucru;
 - dotat dupa caz cu echipament individual de protectie si de lucru.

A4. Seful formatiei de lucru:

- raspunde de stabilirea numarului si nivelului calificarii personalului pentru formatiile de executare a lucrarilor;
- raspunde de elaborarea instructiunilor tehnice de lucru corespunzatoare lucrarilor cuprinse in prezenta conventie;
- ia toate masurile privind evitarea accidentelor de natura neelectrică, precum si a accidentelor de natura electrică;
- raspunde de respectarea de catre personalul propriu a normelor specifice de securitate a muncii, conform sarcinilor si functiilor pe care le detin;

CAIET DE SARCINI

- raspunde de consecintele accidentelor de munca suferite de personalul propriu, precum si de alte persoane, in timpul si imprejurarile specifice lucrarilor executate de personalul propriu in cazul in care acesta se face responsabil pentru aceasta, pe baza cercetarilor efectuate.

A5. Obligatii comune beneficiarului si prestatorului:

- Din punct de vedere administrativ, salariații sunt subordonați unității cu care au semnat contract de muncă;
- Pe toata perioada executiei lucrarilor atat Beneficiarul cat si Prestatorul sunt obligati sa se informeze reciproc asupra problemelor importante de securitate si de sanatate in munca;
- In cazul producerii unui accident de munca partile contractante au obligatia de a nu modifica starea de fapt decat in cazul in care aceasta ar putea genera si alte accidente;
- In cazul producerii unor accidente de muncă, evenimente sau incidente periculoase în activitatea desfasurata, comunicarea, cercetarea și înregistrarea accidentului de munca revine părții contractante care are contract de muncă cu salariatul implicat, respectându-se prevederile Legii nr.319/2006 și Ord. nr. 450/825/2006 privind normele metodologice de aplicare a Legii nr. 346/2002 privind asigurarea pentru accidente de muncă;
- Accidentele de muncă de traseu și accidentele de circulație se trateaza conform legislației de securitate a muncii în vigoare;
- Respectarea de catre partile semnatare a prevederilor din prezenta Conventie constituie pentru acestea o obligatie minimala, fiecareia revenindu-i obligatia de a lua in plus la locurile de munca pe care le organizeaza, cel putin toate masurile tehnice si organizatorice prevazute de legislatia in vigoare, care sa previna eventuale accidente de munca sau alte evenimente.

B. PREVEDERI DE MEDIU**B1. Obligatii comune Beneficiarului si Prestatorului**

- Asigura protectia mediului cu respectarea stricta a legislatiei de mediu nationale si europene in vigoare (gestionarea, transportul si depozitarea deseurilor, biodiversitate, factorii de mediu –apa, aer, sol, substantelor si preparatelor chimice periculoase, zgomot, etc)

B2. Prestatorul are obligatia sa:

- efectueze serviciile/lucrarile doar dupa obtinerea tuturor avizelor de la autoritatile competente (Agentia pentru Protectia Mediului, Administratia Nationala Apele Romane, Natura 2000 etc) dupa caz
- aplice ierarhia deseurilor, in sensul prevenirii generarii deseurilor dupa cum urmeaza: prevenirea, pregatirea pentru reutilizare, reciclarea, alte operatiuni de valorificare, eliminarea;
- colecteze si sa depoziteze selectiv deseurile rezultate din activitatea prestata cu respectarea prevederilor legale;
- transporte deseurile rezultate din serviciile/lucrarile prestate cu respectarea HG 1061/2008;
- predea deseurile rezultate catre agentul economic indicat de Beneficiar in vederea valorificarii/eliminarii acestora;
- asigure toate serviciile/lucrarile necesare remedierii eventualelor prejudicii aduse mediului, din activitatea prestata la Beneficiar, aceste prejudicii fiind consemnate intr-un proces verbal incheiat intre parti;
- ia toate masurile necesare pentru a proteja mediul pe / si in afara locatiei si pentru a evita orice paguba sau neajuns provocat persoanelor, proprietatilor publice sau altora, rezultat din poluare, zgomot sau alti factori generati de metodele sale de lucru si pana la finalizarea serviciilor/lucrarilor;
- asigure toate conditiile cu privire la depozitarea/utilizarea substantelor si preparatelor chimice periculoase, inclusiv instruirea personalului propriu cu privire la prevederile legale si cele din fisa cu date de securitate (FDS)
- dispuna de echipamentul, materialele de decontaminare necesare in caz de accident (doar pentru cazul in care se utilizeaza substante si preparate chimice periculoase);
- informeze imediat APM, ANAR , Beneficiarul si alte autoritati competente despre orice evacuare/emisie de substante si preparate chimice periculoase si sa ia toate masurile necesare pentru reducerea efectelor acestor scurgeri;

CAIET DE SARCINI

- instruiască și să verifice dacă personalul propriu cunoaște și respectă legislația de protecția mediului aplicabilă pentru activitățile desfășurate;
- informeze personalul propriu asupra aspectelor de mediu semnificative în perimetrul în care își desfășoară activitatea;
- mențină în funcțiune un sistem de management de mediu conform SR EN ISO 14001: 2015, dacă a fost solicitat la încheierea contractului.

B3. Se interzice Prestatorului :

- aruncarea sau evacuarea în instalații sanitare ori în rețelele de canalizare a deșeurilor periculoase și/sau a substanțelor și preparatele chimice periculoase;
- să abandoneze deșeurile pe traseu sau să le depoziteze în locuri neautorizate;
- poluarea solului prin scurgeri de carburanți de la utilajele și mijloacele auto folosite;
- spălarea în cursuri de apă sau în lacuri și pe malurile acestora a vehiculelor, a altor utilaje și agregate mecanice, precum și a ambalajelor sau obiectelor care conțin substanțe și preparate chimice periculoase;
- amestecul diferitelor categorii de deșeuri periculoase, precum și al deșeurilor periculoase cu deșeuri nepericuloase;
- efectuarea lucrărilor/serviciilor cu personal care nu a fost instruit și/sau autorizat pentru aceste lucrări.

B4. Beneficiarul are obligația să:

- puna la dispoziția Prestatorului, la cerere, lista privind aspectele de mediu semnificative referitoare la activitatea prestată.

C. PREVEDERI PRIVIND APARAREA ÎMPOTRIVA INCENDIILOR ȘI PROTECTIA CIVILA (SU)**C1. Obligatiile Beneficiarului:**

- Efectuează instructajul introductiv general în domeniul situațiilor de urgență, cu personalul aparținând Prestatorului.

C2. Obligatiile prestatorului:

- Să ia la cunoștință, să-și însușească și să respecte măsurile de apărare împotriva incendiilor, normele și regulile de protecție civilă și prevederile actelor de autoritate emise de conducerea Distribuție Energie Oltenia SA în domeniul situațiilor de urgență, pentru locațiile în care își desfășoară activitatea;
- Să organizeze apărarea împotriva incendiilor la locul de muncă;
- Să respecte normele de apărare împotriva incendiilor, specifice activităților pe care le organizează sau le desfășoară;
- Să participe la instruirea pe Situații de Urgență (SU) specifică personalului din afara unității, conform deciziei în vigoare din Distribuție Energie Oltenia;
- Să instruiască periodic personalul propriu în domeniul Situațiilor de Urgență;
- Să utilizeze numai mijloace tehnice de apărare împotriva incendiilor, certificate conform legii;
- Să întretină și să utilizeze în scopul pentru care au fost realizate mijloacele de apărare împotriva incendiilor puse la dispoziție de beneficiar;
- Să respecte instrucțiunile privind reglementarea fumatului și lucrului cu foc deschis;
Nota : lucrul cu foc deschis se poate permite în cazuri excepționale pe baza de permis de lucru cu foc și aprobare a conducătorului locului de muncă.
Să participe la exercițiile de alarmare-intervenție-evacuare organizate de beneficiar;
Să consemneze în registrele de control ale mijloacelor de apărare împotriva incendiilor lucrările de mentenanță executate, conform cerințelor legale;
- Să aducă la cunoștință beneficiarului, orice defecțiune tehnică ori altă situație care constituie pericol de incendiu;
- Să acționeze, în conformitate cu procedurile stabilite la locul de muncă, în cazul apariției oricărui pericol iminent de incendiu;

CAIET DE SARCINI

- În caz de incendiu trebuie să acorde ajutor când și cât este posibil pentru stingere și înlăturarea efectelor incendiului;
- Să furnizeze beneficiarului toate datele și informațiile de care are cunoștința, referitoare la producerea unor situații de urgență;

C3. Obligații comune ale Beneficiarului și Prestatorului:

- Partile sunt obligate să respecte reglementările tehnice și dispozițiile de apărare împotriva incendiilor și să nu primejduiască, prin deciziile și faptele lor viața, bunurile și mediul;
- Obligațiile cuprinse în convenție sunt minimale. Acestea se completează cu obligațiile care revin beneficiarului și prestatorului din lege.

CAP.V. PREVEDERI FINALE:

- Accesul Prestatorului în locațiile Beneficiarului se face în baza listei cu personalul executant și a legitimațiilor de serviciu;
- Personalul cu drept de control aparținând DEO SA are competența să întrerupă lucrările și să evacueze Prestatorul, dacă constată nerespectarea prevederilor legislației de securitate a muncii sau starea de pericol iminent, cu informarea ulterioară a conducerii Prestatorului;
- Personalul cu drept de control aparținând Prestatorului are acces în sediile DEO S.A pentru controlul formațiilor proprii;
- Înregistrarea accidentelor de muncă se va face de către persoana juridică de care aparține accidentatul, dacă nu s-a stabilit altfel prin procesul - verbal de cercetare a evenimentului. Personalul Prestatorului implicat în evenimente produse în instalațiile electrice are obligația de a da informațiile solicitate de comisia de cercetare a evenimentelor;
- Persoanele cu funcții de conducere a structurilor teritoriale (judetene/regionale) ale Beneficiarului și Prestatorului răspund de aplicarea prevederilor prezentei „Convenții”.

CAP. VI. ANEXE:

Următoarele anexe fac parte integrantă din prezenta Convenție:

- numele și prenumele persoanelor aparținând unității prestatorului /salariatii care lucrează în numele său— Anexa 1;
 - lista categoriilor de lucrări / servicii - Anexa 2;
 - lista personalului ce are dreptul să execute lucrări / servicii – Anexa 3;
 - fișa de instruire colectivă privind sănătatea și securitatea în muncă în conformitate cu HG 1425 / 2006 completată și modificată - Anexa 4;
 - proces verbal de instruire SU a persoanelor din afara unității – anexa 5.
- Încheiat în două exemplare, câte unul pentru fiecare parte, astăzi:

Pentru și în numele Beneficiarului:
Distribuție Energie Oltenia S.A.

Manager DSSM

Pentru și în numele Prestatorului:
Membru al Directoratului

PAGINA CU SEMNĂTURI

Acest document este semnat cu semnătură electronică calificată și/sau cu semnătură electronică avansată furnizată de EVRYO. Pentru verificarea semnăturilor electronice calificate din acest document, *Adobe Acrobat Reader* are deja certificatul Root CA inclus în lista *Trusted Certificates*. Pentru a verifica semnăturile electronice avansate din acest document, trebuie să [downloadați certificatul Root CA](#) și să-l instalați în lista *Trusted Certificates*.

Signature Valid *Advanced*

*Digitally signed by SANDA RADU MIHAI
10004249*

Date: 2026.02.12 17:01:11 +02:00



Signature Valid *Advanced*

*Digitally signed by SANDULESCU CRISTIAN
10004248*

Date: 2026.02.12 17:03:03 +02:00



Signature Valid *Advanced*

*Digitally signed by ROTARU-SIMION
MAGDALENA SILVIA*

Date: 2026.02.12 17:37:03 +02:00



Signature Valid *Advanced*

Digitally signed by ALBA MIRON

Date: 2026.02.12 18:11:03 +02:00



Signature Valid *Advanced*

Digitally signed by BUTOARCA ION EUGEN

Date: 2026.02.13 09:26:02 +02:00

