CONPET S.A., România
Str. Anul 1848 nr. 1-3, Ploieşti, 100559, Prahova
Tel: +40 - 244 - 401360; fax: + 40 – 244 – 516451
CIF: RO 1350020; Cod CAEN 4950; J29/6/22.01.1991
Capital social subscris şi vărsat 28 569 842,40 lei

DGA3

Serviciul IT

22535 / 26.06.2023

Director General Adjunct 3
Radu Necsulescu Digitally signed by Radu Necsulescu Date: 2023.06.26 12:41:40 +03'00'
Ing. Radu Necşulescu

Aprobat în ședința CTE din data:_____

CAIET DE SARCINI

pentru

Achiziționare „Solutie software Data Loss Protection”.

1. **Scop**

Achiziționarea unei solutii software pentru protejarea informatiilor din reteaua informatica a CONPET

2. **Prezentarea generală a lucrării.**

Implementarea unei solutii software DLP (Data Loss Prevention) pentru un număr de 200 de utilizatori ce are ca scop:

- Monitorizarea datelor pe măsură ce acestea se deplasează în interiorul sau în afara organizației
- Protejarea datelor în timp ce acestea sunt manipulate în aplicații, cu controale bazate pe politici care se aliniază proceselor de business
- Identificarea și clasificarea incidentelor cu risc ridicat pentru a ajuta la prevenirea sau remedierea pierderilor de date sau furtul de date.
- Monitorizarea/blocarea transmiterii informatiilor protejate pe diverse canale: mail, dipozitive externe (CD/DVD, USB, etc), FTP sau printare.
- Amprentarea datelor - capacitatea sistemului de a detecta informații sensibile în ciuda manipulării, reformatării sau altor modificări. Amprentele permit protejarea documentelor, integrale sau parțiale și versiuni derivate ale informațiilor protejate, precum și fragmente din informații protejate indiferent dacă sunt tăiate și lipite sau reintroduse.

3. **Cerințe tehnice.**

Soluția propusă va permite detectarea și descoperirea datelor sensibile la nivel de rețea, aplicații și endpoint. Aceasta va fi capabilă de a asigura protecția datelor, împiedicând pierderea / înstrăinarea acestora, prin canalele de comunicare email, web, dar și prin dispozitivele de stocare amovibile. Soluția propusă va fi capabilă să analizeze cum sunt folosite datele de către utilizator, oferind funcții de educare a acestuia pentru a lua deciziile corecte privind stocarea, folosirea și transmiterea datelor sensibile. Totodată, soluția trebuie să fie capabilă sa prioritizeze incidentele de securitate în funcție de riscul pe care îl reprezintă.

Sistemul trebuie să îndeplinească următoarele cerințe si funcționalități:

3.1 Managementul sistemului DLP

3.1.1	Sistemul trebuie să aibă capacitatea de a utiliza o singură politică pentru a scana date ori de câte ori acestea sunt stocate, transmise sau utilizate, atât în rețea, cât și în endpoint si de a aplica automat răspunsul potrivit pentru amenințarea detectată.
3.1.2	Sistemul trebuie să dețină o interfață centralizata pentru editarea politicilor și gestionarea politicilor, pentru toate produsele (în cadrul monitorizării și prevenirii rețelei și al endpoint-ului)
3.1.3	Sistemul trebuie să permită definirea politicilor pe baza oricăruia dintre următoarele: conținut, expeditor/destinatar, caracteristicile fișierului și protocolul de comunicare.
3.1.4	Sistemul trebuie să permită configurarea gravității incidentelor pe baza cantității datelor expuse.
3.1.5	Sistemul trebuie să poată accepta reguli de detectare a includerii și excluderii bazate pe datele din serviciile de directoare pentru a aplica politica bazată pe expeditori și destinatar/destinație
3.1.6	Sistemul trebuie să ofere capabilitatea de a implementa politici de detectare predefinite pentru a acoperi reglementările și cele mai bune practici de detectare, inclusiv dicționare predefinite pentru reglementările specifice industriei/tarii.

3.2 Detecție - General

3.2.1	Sistemul trebuie să ofere capabilități identice de detectare pentru toate amenințările acoperite (de exemplu, atât pentru produsele bazate pe rețea, cât și pentru cele finale, dar și pentru monitorizarea și prevenirea exfiltrării datelor, cât și pentru descoperirea și protecția datelor)
3.2.2	Capacitățile de detectare ale sistemului trebuie să se poată aplica pentru conținutul limbilor europene și asiatice.
3.2.3	Sistemul trebuie să poată inspecta recursiv conținutul arhivelor comprimate (de exemplu ZIP, TAR, RAR) și să detecteze conținutul amprentat
3.2.4	Sistemul trebuie să poată analiza fișierele sau atașamentele foarte mari (20 MB și mai mari) în timpul procesului de detectare a conținutului amprentat.
3.2.5	Sistemul trebuie să fie capabil sa își amintească încălcările utilizatorilor în timp și sa creeze incidente atunci când este atins un prag definit

3.3 Detecție – Amprentarea datelor structurate

3.3.1	Sistemul trebuie să ofere o metodă pentru amprentarea datelor, cum ar fi înregistrările clienților
3.3.2	Sistemul trebuie să ofere conexiune ODBC la baze de date pentru amprentare
3.3.3	Sistemul trebuie să ofere posibilitatea de a limita privilegiile de acces pentru amprentarea datelor structurate.
3.3.4	Sistemul trebuie să ofere unelte / modalități de control pentru a valida precizia unei amprente digitale în momentul creării acesteia
3.3.5	Sistemul trebuie să permită prin metoda de detectare a datelor cu amprentă să fie specificate ce coloane de date constituie o potrivire per-politică
3.3.6	Sistemul trebuie să fie capabil sa facă distincția între diferite tipuri de numere PII. De exemplu, sistemul distinge CNP-ul din 13 cifre al unui client de un număr de telefon din 10 cifre fără prezența unui cuvânt cheie (de exemplu, „CNP”).

3.4 Detecție – Amprentarea datelor nestructurate

3.4.1	Sistemul trebuie să ofere o metodă pentru identificarea și detectarea datelor pe baza exemplelor furnizate în loc să utilizeze amprentele documentului specific
3.4.2	Sistemul trebuie să poată limita privilegiile de acces pentru amprentarea datelor nestructurate.
3.4.3	Sistemul trebuie să ofere măsuri de control pentru a valida precizia unei amprente digitale în momentul creării acesteia
3.4.4	Sistemul trebuie să poată accepta prin metoda de detectare a documentelor cu amprentă găsirea aceluiași text sau a unor porțiuni de text în diferite formate de fișiere. De exemplu, dacă un document cu amprentă este în format Microsoft Word, sistemul va detecta același text care a fost tăiat și lipit direct într-un e-mail.
3.4.5	Sistemul trebuie să poată acceptă potrivirea conținutului unor documente specifice, cum ar fi codul sursă, documentele de marketing sau cele financiare.
3.4.6	Sistemul trebuie să poată acceptă detectarea de versiuni derivate sau tăiate și lipite de conținut care corespund unor documente/paragrafe specifice
3.4.7	Sistemul trebuie permită specificarea de text si expresii șablon care sa poată fi excluse din detecția politicilor si regulilor de DLP
3.4.8	Sistemul trebuie să poată descoperi conținutul serverelor de tip Microsoft Exchange
3.4.9	Sistemul trebuie să poată amprenta fișierele localizate pe servere SharePoint
3.4.10	Sistemul trebuie să poată descoperi conținutul serverelor cloud de tip Microsoft Exchange si SharePoint (Office 365)

3.5 Detecție – Identificarea datelor modelului

3.5.1	Sistemul trebuie să poată detecta conținutul descris în reguli complet personalizabile cu cuvinte și fraze cheie.
3.5.2	Sistemul trebuie să poată detecta conținutul în funcție de potrivirea modelelor cu validările specifice acestuia. In cazul numerelor cardurilor de credit, sistemul trebuie să poată utiliza analize lexicale contextuale, analize statistice ale tiparelor si verificarea „Luhn” pentru a asigura detectarea uni număr de card de credit valid. Prin aceste tehnici sistemul reduce considerabil rezultatele pozitive false pentru tipurile de date care se potrivesc incorect.
3.5.4	Sistemul trebuie să poată detecta prezența transmisiilor sau fișierelor criptate
3.5.5	Sistemul trebuie să poată accepta detectarea pe baza unui anumit tip de document, chiar dacă expeditorul a modificat extensia de fișier
3.5.6	Sistemul trebuie să fie capabil sa detecteze și inspecteze fișierele de imagine utilizând un motor OCR. Este obligatoriu ca motorul OCR să fie încorporat în sistemul DLP.

3.6 Răspuns automat și restricție

3.6.1	Sistemul trebuie să poată trimite alerte prin e-mail
3.6.2	Sistemul trebuie să ofere posibilitatea de a furniza notificări pe ecran utilizatorilor pentru încălcările politicilor pe endpoint-uri.
3.6.3	Acțiunile de răspuns automatizate trebuie să poată fi definite de diferiți parametri, cum ar fi politica încălcată, gravitatea incidentului, numărul de potriviri găsite, protocolul de comunicare utilizat, starea conectată a endpoint-ului și produsul utilizat
3.6.4	Sistemul trebuie să ofere funcționalități de automatizare a fluxului de lucru pentru urmărirea remedierii unui incident (de exemplu, coduri de stare, atribute, cozi de alocare, gravitate etc.)

3.7 Fluxul de lucru pentru răspunsul la incidente

3.7.1	Sistemul trebuie să poată afișa o indicație clară a modului în care transmisia sau fișierul au încălcat politica în incidentul declanșat (nu doar politica care a fost încălcată), inclusiv identificarea clară a conținutului care a motivat potrivirea.
3.7.2	Sistemul trebuie să permită vizualizarea informațiilor de identitate despre expeditor (cum ar fi numele complet, numele managerului, unitatea organizatorică) și destinația transmiterii (de exemplu, date trimise către un blog, chat)
3.7.3	Sistemul trebuie să permită deschiderea atașamentelor originale ale unui eveniment direct din interfața de utilizare
3.7.4	Fiecare utilizator din fluxul de lucru trebuie să poată fi desemnat să remedieze un anumit set de incidente
3.7.5	Gestionarii de incidente trebuie să poată primi notificări automate despre incidentele noi de examinat
3.7.6	Sistemul trebuie să ofere capabilitatea de a defini și urmări un „caz” sau un set de incidente care s-au relaționat după o investigație
3.7.7	Sistemul trebuie să poată exporta cu ușurință un grup de incidente într-un format ușor de citit de o persoană fără acces la sistem (de exemplu, pentru a satisface o cerere de descoperire)
3.7.8	Sistemul trebuie să permită adăugarea de atribute personalizate incidentelor pentru a fi corelate cu procesul de remediere personalizat
3.7.9	Sistemul trebuie să permită ștergerea incidentelor. Această acțiune va fi înregistrată în jurnalul de audit
3.7.10	Sistemul trebuie să poată elibera mai multe incidente din lista în același timp, adică eliberarea mai multor e-mailuri care au fost în carantină.
3.7.11	Sistemul trebuie să poată controla accesul la incidente pe baza rolului și a politicii încălcate
3.7.12	Sistemul trebuie să includă funcția definire a unui rol care nu are drepturi de vizualizare a informațiilor de identitate pentru a proteja confidențialitatea angajaților.
3.7.13	Sistemul trebuie să permită crearea de roluri separate pentru administrarea tehnică a serverelor, administrarea utilizatorilor, crearea și editarea politicilor, remedierea incidentelor și vizualizarea incidentelor pentru date în repaus, în mișcare sau la endpoint.
3.7.14	Soluția trebuie să ofere o metodă de investigare a oricăror modificări neautorizate sau neregulate aduse sistemului (adică modificarea conturilor de utilizator, incidentele de export, crearea de rapoarte). Aceste informații sunt disponibile prin consola de administrare.
3.7.15	Sistemul trebuie să permită ascunderea datelor tranzacțiilor în vizualizarea incidentului.

3.8 Autentificarea utilizatorilor

3.8.1	Sistemul trebuie să permită crearea mai multor utilizatori și atribuirea diferitelor roluri: a. Configurarea unui rol pentru a conține o combinație de permisiuni b. Crearea unui rol pentru a avea acces la funcțiile de administrare a sistemului, dar nu la informații despre politici, incidente sau angajați. c. Crearea unui rol care să permită utilizatorilor să vizualizeze incidente, dar să nu le modifice sau să le remedieze. d. Crearea unui rol care să aibă capacitatea de a vedea rapoarte rezumative, rapoarte de tendințe și valori la nivel înalt fără posibilitatea de a vedea incidente individuale.
3.8.2	Sistemul trebuie să permită ca autentificarea utilizatorului să fie controlată într-un director extern, de ex. Active Directory.
3.8.3	Sistemul trebuie să permită integrarea cu directoare pentru rezolvarea identității expeditorului sau proprietarului fișierului

3.9 Arhitectura distribuită

3.9.1	Arhitectura sistemului trebuie să accepte site-uri la distanță și utilizatori de rețea distribuiți în mai multe locații diferite
3.9.2	Sistemul trebuie să permită configurarea și gestionarea tuturor componentelor de rețea printr-o interfață centralizată
3.9.3	Sistemul trebuie să ofere o capacitate ridicată de disponibilitate/failover

3.10 Managementul sistemului

3.10.1	Sistemul trebuie să ofere rapoarte despre traficul de sistem, performanța și valorile de transfer
3.10.2	Sistemul trebuie să stocheaze datele și jurnalele capturate într-o bază de date centralizată

3.11 Securitatea sistemului

3.11.1	Sistemul trebuie să poată gestiona patch-urile de securitate.
3.11.2	Sistemul trebuie să poată securiza orice legătura de comunicare intre acesta si endpoint-ul pe care rulează agentul.
3.11.3	Fiecare conectare la sistem și modificare a politicilor de sistem sau incidentelor trebuie să fie relatate într-un jurnal de audit

3.12 Integrare

12.1	Sistemul trebuie să permită integrarea nativ cu Web Gateway si sa suporte protocolul ICAP.
12.2	Sistemul trebuie să permită integrare predefinită cu orice sistem de gestionare a cazurilor sau a problemelor
12.3	Sistemul trebuie să permită integrarea cu un gateway de criptare a e-mailurilor
12.4	Sistemul trebuie să permită integrarea cu servere de email exitente
12.5	Sistemul trebuie să permită integrarea cu un instrument de gestionare a incidentelor de securitate (SIEM)

3.13 Raportare și analize

3.13.1	Soluția va include un raport de gestionare a cazurilor pentru detectarea activității utilizatorilor cu risc ridicat sau suspect
3.13.2	Sistemul trebuie să permită filtrarea raporturilor personalizate cu diferite variabile și atribute
3.13.3	Datele de raportare trebuie să poată fi exportate în diverse formate precum PDF, CSV
3.13.4	Rapoartele trebuie să fie partajate în funcție de rol
3.13.5	Utilizatorii sau seturile de utilizatori trebuie să aibă posibilitatea de a se „abona” la seturi de rapoarte de incidente care corespund unor criterii specifice și primesc o livrare programată de e-mail zilnic, săptămânal sau lunar
3.13.6	Sistemul trebuie să poată afișa si tipări rapoartele sub forma unor grafice.
3.13.7	Rapoartele trebuie să poată fi trimise prin e-mail direct din interfața de utilizare fără re-formatare manuală
3.13.8	Sistemul trebuie sa ofere o vizualizare generala de tip „tablou de bord” care poate combina informații din date în mișcare (rețea), date în repaus (stocare) și date la endpoint într-o singură interfață.
3.13.9	Sistemul trebuie să permită vizualizarea detaliata a incidentului dintr-un raport (de tip drilldown). Aceasta caracteristica trebuie să fie posibila datorita interconectării si corelării dintre incidente, politici si rapoarte.
3.13.10	Sistemul trebuie să dețină un set de rapoarte predefinite * Misconduct reports * Security reports * Social Media reports * Data Security reports

3.14 Prevenirea pierderii datelor în rețea

3.14.1	Sistemul trebuie să permită clasificarea traficul în protocoale fără a se baza pe anumite numere de port
3.14.2	Sistemul monitorizează traficul web, inclusiv poșta web, postările web și alte protocoale utilizând HTTP și HTTPS, inclusiv fișiere încărcate
3.14.3	Soluția trebuie să permită monitorizarea /prevenirea imprimării în rețea a informațiilor confidențiale
3.14.4	Sistemul trebuie să poată oferii detalii geografice despre site-ul web pentru a rezolva/clasifica destinația transmisiei HTTP/S
3.14.5	Soluția trebuie să asigure nativ inspecția comunicațiilor SSL
13.4.6	Sistemul trebuie să asigure monitorizarea traficul de mesagerie instantanee

3.15 Prevenirea pierderii datelor prin e-mail

3.15.1	Sistemul trebuie să fie capabil sa blocheaze e-mailurile de ieșire care încalcă politica companiei privind datele confidențiale
3.15.2	Sistemul trebuie să fie capabil sa monitorizeze traficul intern de e-mail, inclusiv atașamentele
3.15.3	Soluția trebuie să utilizeze propriul MTA (Mail Transfer Agent)
3.15.4	Sistemul trebuie să fie capabil sa pună în carantină e-mailurile care încalcă politica companiei privind datele confidențiale
3.15.5	Sistemul trebuie să permită notificarea expeditorilor și administratorilor de securitate despre un e-mail blocat sau pus în carantină

3.16 Prevenirea pierderii datelor prin web

3.16.1	Soluția trebuie să fie capabila să blocheze conștient conținutul transmisiilor de rețea prin HTTP în mod nativ și să furnizeze notificări
3.16.2	Sistemul trebuie să permită blocarea conținutului sensibil pentru a preveni pierderea confidențială a datelor
3.16.3	Sistemul trebuie să includa propriul proxy

3.17 Protecția datelor

3.17.1	Sistemul trebuie să fie capabil sa copieze automat fișiere care încalcă politica
3.17.2	Sistemul trebuie să fie capabil sa pună în carantină și sa șteargă automat fișiere care încalcă politica
3.17.3	Sistemul trebuie să includă o modalitate de a informa proprietarii de fișiere despre fișierele în carantină, inclusiv detalii despre motivul pentru care fișierul a fost pus în carantină. Ex: politica pe care a încălcat-o.

3.18 Informații identificate la scanarea datelor

3.18.1	Sistemul trebuie să fie capabil sa afișeze locația fișierului original și detaliile politicii pe care fișierele le încalcă
3.18.2	Sistemul trebuie să fie capabil sa se integreze cu serviciile de directoare pentru a permite încălcărilor politicii de date în repaus să fie asociate cu o anumită unitate individuală
3.18.3	Sistemul trebuie să furnizeze un singur raport care să acopere datele în repaus în întreaga organizație

3.19 Managementul scanării

3.19.1	Sistemul trebuie să poată oferii o singură interfață de gestionare pentru toate configurațiile și controlul scanării, la nivel de organizație

3.19.2	Sistemul trebuie să lase neschimbat atributul „ultimul accesat” al fișierelor scanate pentru a nu perturba procesele de backup ale organizației
3.19.3	Sistemul trebuie să accepte scanarea repetată programată automat
3.19.4	Sistemul trebuie să accepte scanarea diferențială pentru a reduce volumul de date de scanat
3.19.5	Sistemul trebuie să poată rula mai multe scanări în paralel

3.20 Scalabilitate și securitate

3.20.1	Sistemul trebuie să poata scana locații la distanță cu lățime de bandă redusă
3.20.2	Sistemul trebuie să ofere atât opțiuni de implementare fără agent, cât și pe bază de agent
3.20.3	Comunicațiile dintre sistem și agent trebuie să fie criptate

3.21 Monitorizarea și prevenirea pierderii datelor la nivel de endpoint

3.21.1	Soluția de endpoint trebuie să poata detecta încercările utilizatorilor de a copia date confidențiale pe dispozitive de stocare amovibile (de exemplu, unități USB, dischetă, CD/DVD)
3.21.2	Soluția de endpoint trebuie să poata afișa detalii complete despre incident, inclusiv numele fișierului, informațiile utilizatorului, detaliile potrivirii politicii și o copie a fișierului original care a încălcat politica
3.21.3	Incidentele endpoint-ului trebuie să fie completate într-o interfață centralizată de management/flux de lucru cu incidentele de rețea
3.21.4	Endpoint-ul trebuie să aibă capacitatea de a monitoriza/preveni următoarele: • Taiere/copiere • Lipire • Accesarea fisierului • Captura de ecran • Printare (in retea/ endpoint)
3.21.5	Endpoint-ul trebuie să poată efectua acțiunile pe baza unei anumite aplicații sau grup (de exemplu, tăierea / copierea nu este permisă din Excel)
3.21.6	Endpoint-ul trebuie să fie acceptat cel puțin pe platformele Windows Server 2019 și Windows 10
3.21.7	Soluția trebuie să se poată integra în mod nativ cu soluția de etichetare/clasificare a datelor Boldon James, Azure Information Protection sau echivalent pentru a aplica automat etichete de clasificare a datelor
3.21.8	Soluția trebuie să poată asigura monitorizarea si protecțiea continuă a datelor confidențiale, indiferent dacă utilizatorul se află în interiorul sau în afara rețelei
3.21.9	Soluția trebuie poată monitoriza/proteja utilizatorii la distanță care pot fi deconectați pentru o lungă perioadă de timp sau pot fi conectați numai printr-o conexiune lenta
3.21.10	Soluția de endpoint trebuie să poată proteja conținutul confidențial indiferent de tipul de fișier sau de locația fișierului (de exemplu, face distincția între un document Excel cu date confidențiale care trebuie protejate față de un document Excel fără date confidențiale)
3.21.11	Soluția de endpoint trebuie să poată realiza detectarea bazată pe amprentarea conținutului, chiar dacă endpoint-ul este în afara rețelei
3.21.12	Soluția de endpoint trebuie să poată implementa politici ierarhice de utilizator/grup cu remedieri/răspunsuri configurabile. Aceasta fiind bazata pe informațiile extrase din serviciile de directoare.
3.21.13	Soluția de endpoint trebuie să ofere posibilitatea de a aplica politici pentru informațiile amprentate in afara rețelei
3.21.14	Endpoint-ul trebuie să poată fi configurat prin interfața de gestionare centralizată (împreună cu gestionarea si configurarea rețelei)

3.21.15	Soluția de endpoint trebuie să permită instalarea acesteia pe sisteme de operare precum Microsoft Windows (32/64) si Apple OS X.
3.21.16	Soluția de endpoint trebuie să asigure agentul împotriva manipulării de către utilizatorul final
3.21.17	Endpoint-ul trebuie să includă un bypass local/la distanță
3.21.18	Agentul va trebui sa fie capabil sa efectueze detectarea local, evitând nevoia de a transmite date prin rețea
3.21.19	Scanarea bazată pe agent trebuie să funcționeze și atunci când echipamentul este în afara rețelei
3.21.20	Sistemul trebuie să permită folosirea unei singure politici pentru descoperirea in rețea, cat si pentru descoperirea pe endpoint.
3.21.21	Procesul de descoperire endpoint va include amprente locale
3.21.22	Progresul scanării trebuie să fie raportat la nivel central în timp ce scanările rulează

3.22 Interfață

3.22.1	Soluția trebui sa includă o singură consolă unificată pentru toate operațiunile de configurare și raportare pe toate căile de detectare
3.22.2	Soluția trebuie să permită mai multe conexiuni simultane la sistemul de administrare/raportare
3.22.3	Endpoint-urile trebuie să poată fi configurate cu profiluri diferite pentru diferite grupuri de utilizatori

3.23 Alte cerințe

3.23.1	Prestatorul va asigura instruirea a 10 persoane. Instruirea nu poate dura mai puțin de două zile.
3.23.2	Prestatorul va asigura și următoarele servicii: • Realizarea unui plan de testare – va fi aprobat de reprezentanții CONPET • Instalare soluție DLP • Configurare soluție DLP • Configurare minim 10 endpoint-uri • Testarea funcționalității corecte a soluției
3.23.3	Prestatorul va include în ofertă și eventuale licențe suplimentare necesare funcționării soluției DLP (ex: licențe pentru baze de date)
3.23.4	Prestatorul va asigura calitatea și conformitatea implementării prin folosirea a minim doi specialiști certificați de către producătorul soluției ofertate
3.23.5	Experiența prestatorului va fi exemplificată prin implementarea cu succes a minim 5 proiecte similare dintre care minim unul în domeniul Oil&Gas sau Energie.

Solutia trebuie să asigure descoperirea si protecția datelor sensibile la nivel de rețea, pentru un număr de 200 calculatoare.

Specificațiile tehnice care indică o anumita origine, sursă, productie, 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 „sau echivalent”,

Toate cerințele sunt minimale. Neîndeplinirea integrală a acestora va duce la declararea ofertei ca fiind neconformă.

4. Livrarea.

Livrarea se va face electronic

5. Durata lucrării.

Termenul de implementare este de maxim 90 zile de la semnarea contractului.

6. Garanție.

Se va asigura acces 24x7 la baza de knowledge a producatorului, la sistemul de suport tehnic asistat al producătorului cu timp de răspuns de 45 min pentru incidentele critice, acces la update-uri de produs si upgrade-uri versiuni software, pe o perioada de 3 ani.

Șef Birou Suport Aplicații

Ionela Pînzariu

Ionela Pinzariu Digitally signed by Ionela Pinzariu Date: 2023.06.26 10:10:05 +03'00'

Şef Serviciu IT

Razvan Pop

Razvan-Aurel Pop Semnat digital de Razvan-Aurel Pop Data: 2023.06.26 11:50:43 +03'00'