

## Caiet de sarcini

### pentru Serviciu de mentenanță echipamente informatice din rețeaua IT a Consiliului Județean Cluj

#### 1. Introducere

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

Caietul de sarcini conține, în mod obligatoriu, specificații tehnice. Acestea definesc, după caz și fără a se limita la cele ce urmează, caracteristici referitoare la nivelul calitativ, tehnic și de performanță, siguranța în exploatare, dimensiuni, precum și sisteme de asigurare a calității, terminologie, simboluri, teste și metode de testare, ambalare, etichetare, marcare, condițiile pentru certificarea conformității cu standarde relevante sau altele asemenea.

În cadrul acestei proceduri, U.A.T. Județul Cluj – Consiliul Județean Cluj îndeplinește rolul de autoritate / entitate contractantă, respectiv autoritatea / entitatea contractantă în cadrul Contractului.

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

#### 1. Contextul realizării acestei achiziții

Principalul scop al achiziției îl constituie asigurarea pentru Consiliul Județean Cluj a unui sistem de Servicii integrate de asistență tehnică, întreținere și mentenanță necesar funcționării în condiții optime a întregului sistem informatic.

Echipamentele IT din cadrul Consiliului Județean Cluj se află în 6 locații:

- 2.1. Calea Dorobanților nr. 106 (sediul Consiliului Județean Cluj),
- 2.2. str. Memorandumului nr. 21 (Centrul Național de Informare și Promovare Turistică Cluj CNIPT),
- 2.3. str. Alexandru Vaida Voevod nr. 55 (Direcția de Administrare al Domeniului Public și Privat al Județului Cluj DADPP),
- 2.4. str. Stadionului nr.2 (Direcția de Administrare și Exploatare a Stadionului Cluj Arena DAESA),
- 2.5. str. Aviator Bădescu nr 9 CZPC (Centrul Zonal de Protecție Civilă Cluj-Napoca)
- 2.6. DN1C 18, Rascruci (Castelul Banffy)

#### 2. Serviciul de mentenanță

Activitatea de mentenanță a calculatoarelor și serverelor din rețeaua IT a CJ Cluj presupune asigurarea funcționalității optime a echipamentelor pe 4 nivele:

---

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.

- a. nivel configurare și administrare sisteme (servere și stații de lucru)
- b. nivel configurare și administrare al infrastructurii (firewall, conexiuni VPN, routere, switch-uri și wireless Access Points (AP))
- c. nivel securitate (analiză, detecție și prevenire a infectării cu malware a echipamentelor din cadrul rețelei IT precum și analiză, detecție și prevenire a posibilelor vulnerabilități în ceea ce privește accesul neautorizat la elementele rețelei IT a CJ Cluj.
- d. nivel conigurare și administrare echipamente sala de ședințe (echipamente audio-video, compensator de sunet, mixer audio, integrare streaming, creare proceduri de vot, arhivare ședințe, streaming online).
- e. nivel configurare și administrare centrala telefonica IP si telefoane IP.
- f. nivel instalare, configurare și administrare stații de lucru (sisteme de operare, semnături electronice, software, hardware).

Având în vedere ca infrastructură IT a instituției este de un nivel de complexitate operațională ridicat, integrând un ecosistem avansat de securitate și conectivitate bazat pe tehnologia Cisco și soluții de tip Unified Threat Management (UTM) / Next-Generation Firewall (NGFW). Această arhitectură asigură o protecție superioară a rețelei cibernetice prin funcții integrate de firewall, scanare antivirus, IPS, filtrare URL și controlul a peste 3000 de aplicații, permițând monitorizarea granulară a traficului pe bază de utilizator și/sau locație geografică. Conectivitatea este garantată printr-o topologie redundantă de tip High Availability (HA) Activ-Activ, susținută de echipamente core de tip data center cu capacitate de switching de minim 1760 Gbps și tehnologie MCLAG pentru o reziliență maximă și zero downtime în operare. Segmentul de stocare și backup este consolidat prin tehnologia NetApp, oferind un mediu scalabil ce utilizează deduplicarea și compresia inteligentă a datelor pentru eficiență optimă. Securitatea datelor este întărită prin mecanisme de replicare sincronă și asincronă, asigurând continuitatea operațională și recuperarea rapidă în caz de dezastru, inclusiv prin integrarea cu medii multi-cloud. Ecosistemul de comunicare și colaborare de tip paperless, furnizat de către producătorul ITC, este integrat nativ în noua infrastructură, facilitând fluxuri de lucru digitale și accesul instantaneu la informații prin sisteme Videowall de mari dimensiuni și stații grafice profesionale cu monitoare, pentru monitorizarea permanentă a stării de securitate; sisteme dedicate de tip *paperless* pentru delegați, cu partajare electronică securizată a documentelor; soluție audio HiFi și transmisii audio-video online criptate; tehnologie de video tracking și o acoperire extinsă a rețelei wireless prin 104 puncte de acces Wi-Fi 6 (enterprise class), cu autentificare securizată WPA3.

Managementul întregului sistem este centralizat printr-un server de jurnalizare capabil să gestioneze 25 GB de log-uri zilnic, oferind un panou de control unificat pentru orchestrarea și răspunsul incidentelor de securitate. Având în vedere acest nivel ridicat de complexitate tehnologică, este imperativ ca ofertantul să demonstreze capacitatea profesională documentată a companiei și să desemneze un număr minim de trei specialiști calificați pentru asigurarea mentenanței acestui mediu critic.

---

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.

Prezența ecosistemului Microsoft 365, în cadrul instituției, reprezintă un pilon strategic în arhitectura digitală a instituției, asigurând continuitatea fluxurilor de lucru și a comunicării critice. Având în vedere că instituția gestionează un număr de 340 conturi de utilizator, integrarea nativă a acestora cu serverul de e-mail Exchange și portalul de politici de securitate Microsoft Entra este esențială pentru menținerea unui mediu de lucru securizat și eficient. Administrarea acestui mediu complex presupune gestionarea avansată a identităților digitale și implementarea unor politici riguroase de Acces Condiționat (Conditional Access), menite să protejeze datele sensibile împotriva accesului neautorizat. În contextul infrastructurii IT, aceste servicii cloud sunt corelate cu sistemele de securitate cibernetică, care asigură vizibilitatea și controlul traficului pentru peste 3.000 de aplicații. Monitorizarea centralizată a accesului și a log-urilor de autentificare este realizată prin serverul dedicat de jurnalizare, capabil să proceseze un volum de 25 GB de date zilnic, oferind un panou de control unificat pentru detectarea amenințărilor în timp real.

Pentru a garanta funcționarea optimă, reziliența și conformitatea întregii infrastructuri, este imperativ ca personalul responsabil cu mentenanța să dețină certificări recunoscute de către producătorii echipamentelor și sau furnizorii serviciilor integrate în infrastructura instituției.

Astfel, expertiza certificată a echipei de suport reprezintă garanția unei administrări profesionale a identităților și a protecției datelor, asigurând un mediu digital stabil și protejat împotriva celor mai recente amenințări cibernetică.

Prezentarea certificărilor solicitate este esențială, nu doar pentru a valida competențele tehnice necesare administrării infrastructurii, ci și pentru a asigura respectarea condițiilor de garanție impuse de producătorii echipamentelor. În acest context, specialiștii desemnați trebuie să dețină în mod obligatoriu, cumulat, certificările menționate mai jos:

- **Certificare** pentru instalarea de soluții de cablare structurată de la un producător european de conectică și cabluri de cupru și fibră optică;
- **Certificare Microsoft MS-900 / Microsoft 365 Fundamental** – deținerea de competențe fundamentale privind utilizarea și administrarea ecosistemului Microsoft 365 și ale serviciilor cloud asociate.
- **Certificare CCIE Enterprise Infrastructure** – deținerea de competențe privind planificarea, implementarea, verificarea și depanarea rețelelor de comunicații, dovedite prin prezentarea unei diplome/ certificări în domeniu recunoscută la nivel național/ internațional.
- **Certificare CCIE Security** - deținerea de competențe avansate privind proiectarea, implementarea, administrarea și securizarea infrastructurilor de rețea, inclusiv identificarea și remediarea vulnerabilităților, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.
- **Certificare SMBE 700-750** – deținerea de competențe privind proiectarea, implementarea și administrarea soluțiilor de rețea și securitate pentru

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.

întreprinderi mici și mijlocii, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

- **Certificare CCNP Enterprise** – deținerea de competențe avansate privind proiectarea, implementarea, configurarea și depanarea rețelelor de comunicații complexe la nivel enterprise, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.
- **Certificare CCNP Security** – deținerea de competențe avansate privind proiectarea, implementarea, configurarea și gestionarea soluțiilor de securitate a rețelelor, incluzând protecția infrastructurii, detecția amenințărilor și răspunsul la incidente, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.
- **Certificare Cisco Certified Specialist – Enterprise Design** – deținerea de competențe privind proiectarea arhitecturilor de rețea la nivel enterprise, incluzând soluții avansate de conectivitate, securitate și optimizare a performanței, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.
- **Certificare Cisco Certified Specialist – Network Security Firepower** – deținerea de competențe privind implementarea, configurarea, administrarea și optimizarea soluțiilor de securitate Cisco Firepower, incluzând protecția împotriva amenințărilor, politica de securitate și gestionarea evenimentelor, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.
- **Certificare NetApp Certified Data Administrator, ONTAP** – deținerea de competențe avansate privind administrarea și gestionarea soluțiilor de stocare și protecția datelor utilizând sistemul ONTAP de la NetApp, incluzând configurarea, monitorizarea și optimizarea performanței, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.
- **Certificare NetApp Certified Hybrid Cloud Administrator** – deținerea de competențe avansate în administrarea soluțiilor de stocare și management al datelor într-un mediu de cloud hibrid, utilizând tehnologiile NetApp pentru integrarea și gestionarea datelor între infrastructuri on-premises și cloud, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.
- **Certificare NetApp Certified Implementation Engineer - SAN Specialist, ONTAP** – deținerea de competențe avansate privind implementarea, configurarea și administrarea soluțiilor SAN (Storage Area Network) utilizând tehnologia ONTAP de la NetApp, incluzând designul, gestionarea și optimizarea performanței infrastructurii de stocare, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.
- **Certificare NetApp Certified Support Engineer** – deținerea de competențe avansate în furnizarea de suport tehnic pentru soluțiile de stocare NetApp, incluzând diagnosticarea, depanarea și rezolvarea problemelor legate de hardware și software, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.

---

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.



- Certificare NetApp Certified Storage Installation Engineer, ONTAP – deținerea de competențe avansate în instalarea, configurarea și implementarea soluțiilor de stocare NetApp utilizând tehnologia ONTAP, incluzând configurarea hardware-ului, integrările cu rețelele de stocare și optimizarea performanței, dovedite prin prezentarea unei diplome/certificări în domeniu recunoscută la nivel național/internațional.
- Certificare ITC - Apointed Authorized Professional Installer & Maintenance Service Provider– atestă competențe de specialitate în instalarea profesională și furnizarea de servicii de întreținere pentru soluțiile ITC recunoscute oficial. Această certificare demonstrează abilități în configurarea și mentenanța echipamentelor și infrastructurilor IT, conforme cu standardele industriei.
- Microsoft 365 Certified: Endpoint Administrator Associate - deținerea de competențe avansate de gestionarea dispozitivelor finale. Specialistul este responsabil pentru securizarea acestora, implementarea politicilor de conformitate, gestionarea aplicațiilor și protejarea datelor pe toate stațiile de lucru care accesează resursele instituției.
- Microsoft Certified: Information Protection and Compliance Administrator Associate - deținerea de competențe avansate de protejare a datelor sensibile și gestionarea riscurilor. Specialistul implementează soluții de prevenire a pierderilor de date (DLP), clasificarea informațiilor și politici de retenție, asigurându-se că documentele instituției rămân confidențiale și conforme cu reglementările legale (cum ar fi GDPR).
- Microsoft Certified: Power Platform Solution Architect Expert - deținerea de competențe avansate complexe de automatizare și analiză a datelor, cu rol de a asigura că aplicațiile personalizate și fluxurile de lucru digitale ale instituției sunt scalabile, sigure și integrate perfect cu restul ecosistemului IT.
- Microsoft Certified: Cybersecurity Architect Expert - deținerea de competențe avansate de arhitectura globală de securitate, definind strategiile de apărare împotriva atacurilor cibernetice, protejarea identităților și securizarea infrastructurii hibride (cloud și on-premises).
- Microsoft Certified: Identity and Access Administrator Associate - deținerea de competențe avansate de gestionare a portalului Microsoft Entra (Azure AD), controlul accesului securizat utilizatorilor la resurse, acces condiționat (Conditional Access) și gestionarea corectă a identităților.
- Microsoft 365 Certified: Administrator Expert - deținerea de competențe avansate de expertiză pentru ecosistemul Microsoft 365 și integrarea lor strategică, performanța sistemului și suportul tehnic de nivel avansat pentru întreaga infrastructură.

Având în vedere complexitatea tehnologică a noii infrastructuri implementate, care integrează soluții de ultimă generație de la lideri globali precum Cisco, NetApp și Microsoft, asigurarea unei mentenanțe de înalt nivel nu reprezintă doar o opțiune operațională, ci o necesitate strategică și o obligație de conformitate. Nivelul de interconectare dintre ecosistemul de colaborare paperless, stocarea hibridă de date și securitatea cibernetică impune ca echipa tehnică să dețină competențe validate

---

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.



oficial. Deținerea cumulativă a certificărilor solicitate este obligatorie din următoarele considerente fundamentale:

- Garantarea Rezilienței și Continuității Operaționale (Cisco & NetApp)

Prezența experților certificați CCIE (Enterprise & Security) și CCNP garantează că arhitectura de rețea, capabilă de un switching de 1760 Gbps, este administrată la standarde de "Zero Downtime". Certificările NetApp (ONTAP, SAN, Hybrid Cloud) sunt vitale pentru gestionarea volumelor masive de date, asigurând că replicarea sincronă și recuperarea în caz de dezastru (Disaster Recovery) sunt configurate corect, protejând instituția împotriva pierderilor de date critice.

- Securitate Avansată și Protecția Identității (Microsoft & Cisco Firepower)

Într-un mediu cu 340 conturi Microsoft 365 din care 24 au servicii în plus față de Business Standard integrate cu Microsoft Entra, riscurile cibernetice sunt gestionate prin politici de Acces Condiționat și MFA. Certificările de tip Cybersecurity Architect Expert și Identity and Access Administrator asigură că identitățile utilizatorilor și accesul la date sunt protejate prin mecanisme de apărare proactivă. Simultan, experții în Cisco Firepower oferă bariera perimetrală necesară pentru filtrarea a peste 3000 de aplicații și monitorizarea traficului la nivel geografic.

- Conformitate, Garanție și Standarde Europene

Solicitarea certificărilor pentru cablare structurată (producător european) și ITC Authorized Provider derivă din necesitatea de a respecta condițiile de garanție extinsă ale echipamentelor. O intervenție neautorizată sau realizată de personal necertificat poate duce la pierderea suportului tehnic din partea producătorului și la degradarea performanței întregului ecosistem.

- Eficiență Digitală și Automatizare (Power Platform & Endpoint Admin)

Tranziția către un mediu complet digital și paperless necesită specialiști capabili să proiecteze fluxuri de lucru scalabile (Power Platform Solution Architect) și să securizeze toate dispozitivele finale ale delegaților (Endpoint Administrator), asigurând o experiență de utilizare fluidă și sigură.

În contextul evoluției tehnologice rapide și al necesității de a asigura un cadru operațional eficient, instituția noastră se confruntă cu provocări semnificative în gestionarea infrastructurii IT, având în vedere lipsa unui departament IT intern specializat. În acest sens, cerințele impuse prin caietul de sarcini, inclusiv certificările solicitate, sunt fundamentale și obligatorii pentru garantarea unui nivel optim de securitate, funcționalitate și continuitate a activităților instituționale.

Experiențele anterioare au demonstrat că externalizarea serviciilor IT către furnizori, firme, prestatori, operatori economici care nu dețineau competențele și certificările necesare a generat dificultăți majore în administrarea rețelei și a sistemelor IT.

Aceste dificultăți nu doar că au afectat fluxul operațional zilnic, dar au dus și la atacuri cibernetice și atacuri ale sistemelor informatice, inclusiv ale site-ului web al instituției, cauzate de vulnerabilitățile generate de lipsa pregătirii corespunzătoare a furnizorilor anteriori.

---

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.

Printre problemele semnalate s-au numărat deficiențe în mentenanța sistemelor informatice, întâzieri în remedierea incidentelor critice și vulnerabilități în ceea ce privește securitatea cibernetică.

Mai mult decât atât, deficiențele în administrarea infrastructurii IT au avut un impact negativ asupra organizării și desfășurării ședințelor Consiliului Județean, generând întâzieri, dificultăți tehnice și, implicit, afectând procesul decizional și activitatea administrației. Aceste probleme au evidențiat necesitatea stringentă de a colabora cu furnizori care dispun de expertiza necesară, certificată prin standarde recunoscute la nivel național și internațional.

Având în vedere importanța strategică a unei infrastructurii IT fiabile și sigure, impunerea unor cerințe riguroase în ceea ce privește calificările și certificările furnizorilor este esențială. Doar prin respectarea acestor criterii se poate asigura un nivel adecvat de profesionalism, prevenirea unor riscuri operaționale semnificative și menținerea unui standard ridicat al serviciilor IT oferite instituției.

Prin urmare, justificăm necesitatea respectării acestor cerințe ca fiind esențială pentru eficiența, securitatea și continuitatea activității instituției noastre, reducând riscurile asociate unor eventuale disfuncționalități și optimizând procesele administrative și decizionale.

## 2.1 Activitatea de mentenanță va avea urmatoarele 5 directii:

### 2.1.1 Mentanța și administrarea infrastructurii rețelei

Pentru servere, prestatorul va asigura, împreună cu persoana de specialitate, gestionarea hardware și administrarea software completă împreună cu activitatea de salvare/restaurare sisteme informatice și date. Accesarea echipamentelor se poate realiza din sala serverelor a Consiliului Județean Cluj.

Toata activitatea se va derula în colaborare cu personalul de specialitate desemnat de către CJC, care vor furniza informațiile necesare.

Prestatorul va asigura administrarea serverelor existente (onsite și/sau remote), care implică realizarea a cel puțin următoarelor operații :

- a. Instalarea, upgradarea, configurarea sistemului de operare pe toate serverele;
- b. Monitorizarea / efectuarea update-urilor de securitate;
- c. Monitorizarea / efectuarea update-urilor programelor antivirus;
- d. Configurarea politicii de backup prin Serverul de backup, conform cerințelor stabilite de responsabilul IT;
- e. Restaurarea în cazul unui dezastru a sistemului de operare și a informațiilor, dând un timp de realizare a restaurării;
- f. Asistenta tehnica pentru administratorul de sistem local/responsabilul IT in problemele curente de administrare;

Firma Prestatoare va asigura instalarea update-urilor, în cel mai scurt timp posibil, nu mai mult de 30 zile după apariția acestora, la toate serverele existente.

Pentru stații de lucru:

- a. Configurarea sistemelor de operare la toate stațiile de lucru;

---

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.

- b. Intervenția în cazul apariției unor disfuncționalități ale stațiilor, în vederea diagnosticării defectului hard sau soft;
- c. Testarea tuturor componentelor hard ale calculatorului pentru a se verifica funcționarea lor corectă, unitară, fără conflicte între subansamble;
- d. Optimizarea funcționării stațiilor;
- e. Upgrade-uri hardware sau software la cererea persoanei de specialitate din cadrul CJC;
- f. Asistență tehnică pentru administratorul de sistem local în problemele curente de administrare

Operațiunile menționate sunt obligatorii pentru toate stațiile de lucru și serverele din cele șase locații, precum și pentru cele care vor fi instalate pe durata contractului. Verificarea periodică a parametrilor tehnico-funcționali ai traseelor de rețea precum și a echipamentelor de conectare, cu aparatură specializată FLUKE sau similară ca și performanțe.

Mentenanța și administrarea va cuprinde echipamentele din locațiile:

**Sediul Consiliului Județean Cluj, str. Dorobanților nr. 106**

- Se va asigura administrarea Cisco Secure Firewall 3105 NGFW Appliance – 2 bucăți
- Se va asigura administrarea serverelor Cisco HV-NODE-PROD-01 – 8 bucăți
- Se va asigura administrarea serverelor virtuale – 8 bucăți
- Se va asigura administrarea serverului de backup – 1 buc.
- Se va asigura administrarea AD – 1 buc.
- Se va asigura administrarea stațiilor de lucru – **215 buc.**
- Se va asigura administrarea soluției de securitate Cisco ASA cu Firepower
- Se va asigura administrarea switchurilor Cisco Meraki MS225-24 L2 Stck Cld-Mngd 24x GigE Switch – 23 bucăți
- Se va asigura administrarea switchurilor Cisco Meraki MSS 210-24 – 7 bucăți
- Se va asigura administrarea switchurilor Cisco Meraki MS225-24P L2 Stck Cld-Mngd 24x GigE 370W PoE Switch – 2 bucăți
- Se va asigura administrarea routerelor Cisco Meraki MX68 Router/Security Appliance – 2 bucăți
- Se va asigura administrarea switchurilor Nexus 9300 48p 1/10/25G, 6p 40/100G, MACsec, SyncE – 2 bucăți
- Se va asigura administrarea AP-urilor Cisco Meraki MR36H Wi-Fi 6 Cloud Managed AP – 47 bucăți
- Se va asigura administrarea AP-urilor Cisco Meraki MR44 WiFi 6 Indoor AP – 55 bucăți
- Se va asigura administrarea AP-urilor Cisco Meraki MR33 WiFi 6 Indoor AP – 55 bucăți
- Se va asigura administrarea AP-urilor Cisco Catalyst 9162I AP (W6E, tri-band 2x2) w/Meraki – 6 bucăți
- Se va asigura administrarea soluției complete de conferință paperless, a sistemului audio, videwall-uri, servere de conferință, sisteme de video tracking

---

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.

si camerele video, consolele digitale si ecranele escamotabile, serverul de streaming video.

- Se va asigura administrarea centralei de telefonie VoIP – 1 buc.
- Se va asigura administrarea posturilor telefonice – 80 buc.
- Nod de alimentare 6000w – 5 buc.
- UPS (1500VA, 1350W) – 26 buc
- Se va asigura administrarea tuturor licențelor software, licențelor pentru echipamente și orice alte licențe utilizate in cadrul instituției.

#### **Direcția de Administrare a Domeniului Public și Privat – Str. Al Vaida Voievod**

- Se va asigura administrarea routerelor Cisco Meraki MX68 Router/Security Appliance – 2 bucăți
- Se va asigura administrarea switchurilor Meraki MSS 210-24 – 2 bucăți
- Se va asigura administrarea switchurilor Meraki MSS 210-48 – 1 bucăți
- UPS (1500VA, 1350W) – 2 buc.
- Se va asigura administrarea WAP – 6 bucăți
- Se va asigura administrarea stațiilor de lucru – 50 buc.

#### **Direcția DAESCA-Stadionul Cluj Arena**

- Se va asigura administrarea routerelor Cisco Meraki MX68 Router/Security Appliance – 1 bucată
- Se va asigura administrarea switchurilor HP Procurve – 15 bucăți
- Se va asigura administrarea stațiilor de lucru – 25 buc.

#### **Centrul Național de Informare și Promovare Turistică Cluj CNIPT**

- Se va asigura administrarea routerelor Cisco Meraki MX68 Router/Security Appliance – 1 bucată
- Se va asigura administrarea WAP 1 buc.
- Se va asigura administrarea stațiilor de lucru – 5 buc.

#### **Castelul Banffy**

- Se va asigura administrarea rețelei de date – 1 buc.
- Se va asigura administrarea stațiilor de lucru – 6 buc.

#### **Centrul Zonal de Protecție Civilă Cluj-Napoca**

- Se va asigura administrarea rețelei de date – 1 buc.

Se va urmări, de către firma prestatoare, a licențelor și termenelor de garanție pentru echipamentele de rețea care au licențe pe baza de abonament. Pentru reînnoirea licențelor care urmează să expire, prestatorul va face o notificare cu 30 de zile înainte. Pe lângă echipamentele menționate, contractul va include toate celelalte echipamente care fac parte din infrastructura rețelei, precum și cele ce vor fi instalate pe durata derulării acestuia.

### **2.1.2 Asigurarea prelungirii serviciului Microsoft Office 365 Business**

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.

Prestatorul va ofera în cadrul contractului de mentenanță costul pe un an a 340 conturi Microsoft 365 cu abonament Microsoft 365 E3.

### 2.1.3 Echipamente, licențe, licențe pentru servicii de securitate, piese de schimb și accesorii

Prestatorul va asigura pe perioada de valabilitate a contractului echipamente-piese de schimb și accesorii prevăzute în Anexa 1. Echipamentele, accesorii, piesele sau subansamblele achiziționate și care vor completa sau le vor înlocui pe cele defecte vor avea o perioadă de garanție minimă de 12 luni. Piesele de schimb și echipamentele prevăzute în Anexa 1, care intră sub incidența acestui contract, se vor putea achiziționa separat în baza unor *devize* întocmite de prestator, dar numai cu acceptul achizitorului, în limita fondurilor alocate pentru acest lucru.

Reprezentantul prestatorului va emite un *deviz*, care va cuprinde, modelul și seria echipamentului ce necesită înlocuire de piese, înlocuire totală sau adaugare, locația, tipul și costul componentelor necesare. Montarea sau înlocuirea efectivă a pieselor/echipamentelor, după caz, va fi făcută NUMAI după aprobarea devizului de către personalul de specialitate desemnat de CJC. Transportul, ambalajul, alte cheltuieli și comisioane angajate de furnizor vor fi incluse în prețul produselor.

### 2.1.4 Mentanța și administrarea echipamentelor din sala de ședință

Prestatorul va asigura pe perioada de valabilitate a contractului patch-uri de securitate, actualizarile software cu cele mai recente versiuni certificate de către producătorul echipamentelor, mentenanța sistemului audio-video integrat, sincronizarea sistemului video cu microfoanele active, mentenanța tehnico-mecanică a sistemelor de elevare a ecranelor paperless, mentenanța serverului de live streaming, a sistemelor software complexe de realizare a procedurilor de vot și asigurarea tuturor cerințelor de securitate pentru acestea. Acestea se vor realiza numai în baza procedurilor de service certificate de către producător și prin utilizarea numai a componentelor, subansamblelor originale.

### 2.1.5 Mentanța și administrarea echipamentelor de telefonie IP

Prestatorul va asigura, pe întreaga durată a contractului, implementarea patch-urilor de securitate și actualizarea software-ului echipamentelor de telefonie IP la cele mai recente versiuni certificate de către producător. De asemenea, va efectua mentenanța infrastructurii de telefonie IP, asigurând funcționarea optimă a serverelor de comunicație, a gateway-urilor VoIP, a telefoanelor IP și a altor echipamente asociate.

Prestatorul va garanta sincronizarea și integrarea corespunzătoare a sistemului de telefonie IP cu infrastructura IT existentă, precum și menținerea standardelor de securitate cibernetică, inclusiv protecția împotriva accesului neautorizat și a vulnerabilităților de rețea.

---

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.



Toate operațiunile de întreținere și actualizare se vor desfășura exclusiv conform procedurilor de service certificate de către producător și prin utilizarea componentelor și subansamblelor originale.

## 2.2 Suport tehnic

Solicitarea privind remedierea unui defect hard sau soft se va realiza și printr-un sistem de ticketing, astfel încât toți specialiștii implicați în această activitate vor fi înștiințați prin email la adăugarea unui tichet de intervenție.

Pentru monitorizarea procesului de remediere al problemelor apărute se definesc:

*Timpul de intervenție* - timpul de la înregistrarea problemei până la sosirea specialiștilor în locație.

*Timpul de rezolvare* - timpul de la intervenție până la soluționare problemei.

Se definesc de asemenea, 2 nivele de severitate pentru probleme:

**Severitate 1** - o problemă care afectează funcționarea unuia dintre serverele Consiliului Județean Cluj sau o problemă legată de accesul la Internet .

**Severitate 2** - o problemă care afectează funcționarea Sistemului informatic, cum ar fi: stațiile de lucru, elemente active de rețea, conecțică, etc.

Timpii de intervenție și rezolvare a apelurilor recepționate prin telefon sau fax de la Consiliul Județean Cluj, se vor încadra în limitele specificate mai jos:

Grad de severitate	Timp de intervenție	Timp de rezolvare
Severitate 1	20 min	maxim 2 ore
Severitate 2	1,5 ore	maxim 24 de ore

Numai în cazul în care diagnosticarea sau remedierea nu se poate face pe loc sau în cadrul timpilor maximi de rezolvare specificați sau piesa de schimb necesară nu este disponibilă, echipamentul defect este retras pentru a fi reparat în laboratorul firmei prestatoare.

Indiferent unde a fost efectuată depanarea echipamentului sau modul în care s-a realizat depanarea, echipamentul reparat va fi testat în locația rețelei Consiliului Județean Cluj, în prezența personalului de specialitate desemnat de CJC, pentru a se verifica starea de bună funcționare.

Remedierea, înlocuirea componentelor hardware în pană sau adăugarea celor noi se va face la cererea persoanei de specialitate desemnate din cadrul C.J.C. Orice acțiune de acest gen se va consemna într-un registru, prezent în dublu exemplar, atât la sediul administrativ al Consiliului Județean Cluj, cât și la cel al prestatorului.

În urma remedierii defectului hard sau soft, predarea echipamentului în stare funcționabilă se face către administratorul rețelei de calculatoare a CJC.

În mod curent, remedierea unui defect hard nu trebuie să depășească 2 ore iar a celui soft 3 ore de intervenție.

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.

Toate intervențiile vor fi făcute doar cu acordul și înștiințarea prealabilă a responsabilului IT din cadrul CJC. Toate intervențiile care necesită demontarea carcasei se vor realiza pe răspunderea firmei prestatoare, sub supravegherea responsabilului IT din cadrul Consiliului Județean Cluj.

Toate înlocuirile de subansamble sau adăugarea celor noi, chiar dacă sunt *plug and play* se vor realiza de către specialiștii firmei prestatoare sau de persoana de specialitate din cadrul Consiliului Județean Cluj.

Operațiile amintite la punctul anterior, implică și instalările de produse soft aditionale (de ex. drivere) aferente subansamblelor înlocuite.

Activitatea de service include și punerea în funcțiune, configurarea și instalarea pieselor de schimb și a licențelor și a software-ului achiziționat în cadrul acestui contract (Microsoft Office) care trebuie montate, configurate, împreună cu celelalte operații care trebuie efectuate asupra echipamentelor în care vin instalate.

Firma prestatoare va asigura nivelul de compatibilitate a suitei Microsoft Office prin instalarea unitară a ultimei variante (2026) pe toate stațiile de lucru din cadrul Consiliului Județean Cluj, precum și deinstalarea versiunilor mai vechi acolo unde este necesar acest lucru.

Toate solicitările de intervenție în locație pentru acțiuni corective, cu datele lor de identificare și cu soluțiile oferite, vor fi înregistrate pe un formular specific care va fi completat în locație și pe care se va menționa în mod special starea sistemului la sfârșitul intervenției.

La sfârșitul fiecărei luni, se va realiza un raport centralizator cu informații explicite, extrase din sistemul de tichete de intervenție, asupra tuturor operațiilor, activităților, intervențiilor etc. efectuate în sistem. Personalul de specialitate desemnat de către CJC va verifica corespondența informațiilor de pe fișele de intervenție și raportul centralizator corespunzător aceleiași luni.

Raportul centralizator corespunzător semnat de specialistul firmei prestatoare și avizat de persoana de specialitate din cadrul CJC va fi atașat facturii lunare de plată a service-ului pentru achitarea contravalorii serviciilor, acesta va include informații despre prestator și beneficiar, luna de referință a raportului, identificarea facturii de servicii a carei anexa este raportul, numărul de tichete întocmite și detaliile complete ale acestora (descrierea defectului, intervenției și data acesteia). Pentru analiza corectă a datelor, fiecare raport va conține și o analiză statistică a intervențiilor pentru ultimele 90 de zile precum și distribuția acestora pe fiecare direcție/subordonată și continuată în contractul de mentenanță.

Toate materialele de întreținere / reparare (aspiratoare praf, pensule, substanțe degresante, spray, etc.) și toate mijloacele tehnice sunt asigurate de către ofertant și sunt incluse în cadrul valorii lunare ale contractului (în propunerea financiară).

În cadrul activității de reparații, devizul de plată se va întocmi numai pentru contravaloarea componentei în cauză, contravaloarea manoperei de instalare fiind inclusă în contractul de servicii.

Firma prestatoare se va angaja să păstreze confidențialitatea tuturor datelor la care are acces.

---

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.

### 3. Atribuțiile și responsabilitățile părților

Durata contractului: de la data 01.05.2026 și până la data de 31.12.2026, cu posibilitatea prelungirii pe încă maxim 4 luni, până la data de 30.04.2027

Tarifele vor îngloba cheltuielile pentru prestarea întregii game de servicii hardware și software aferente fiecărui echipament în parte.

Serviciile care vor fi achiziționate de către autoritatea contractantă în timpul derulării contractului de servicii vor face automat obiectul acestui contract, fără a se majora prețul contractului.

Echipamentele care vor fi scoase din funcțiune în timpul derulării contractului nu vor diminua prețul contractului.

Activitățile desfășurate în cadrul serviciilor solicitate se vor desfășura pe toată durata contractului, fără discontinuități.

Toate activitățile desfășurate de Prestatorul de servicii vor trebui să se încadreze în politica generală a Consiliului Județean Cluj privind gestionarea unui sistem informatic operațional, eficient și coerent și menținerea deschiderii către perfecționarea continuă a sistemului Informatic în conformitate cu strategia Consiliului Județean.

Transportul echipamentelor și specialiștilor, de la sediul firmei prestatoare sau între sediile Beneficiarului se realizează în exclusivitate pe cheltuiala firmei prestatoare.

Garanția oferită pentru piesele de schimb și pentru manoperă va fi de cel puțin 90 de zile.

Personalul de specialitate desemnat de CJC va asigura accesul personalului firmei prestatoare în sediul Consiliului Județean și va supraveghea toată activitatea depusă.

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

#### 3.1 Ofertantul (prestatorul) are următoarele obligații principale:

- a. Prestatorul trebuie să asigure, împreună cu personalul specializat al C.J.C., configurarea și funcționarea optimă a sistemului informatic al Consiliului Județean Cluj.
- b. Prestatorul trebuie să efectueze activitatea de service hard și soft asupra tuturor componentelor care alcătuiesc rețeaua astfel încât fiecare element component al structurii să funcționeze optim.
- c. Activitatea de service și asistență tehnică hardware și software se va derula sub directă îndrumare a personalului de specialitate desemnat de Consiliul Județean Cluj care va coordona activitatea de prestare a service-ului.
- d. Ofertantul va trebui să demonstreze că are un punct de lucru operațional în Cluj-Napoca
- e. Ofertantul va avea obligația să mobilizeze cei 3 specialiști desemnați, la nevoie 4, la sediul CJ Cluj din Calea Dorobanților nr. 106, 8 ore /zi, în intervalul orar 7.30-16 de luni până joi și 7.30-13.30 vineri 40 de ore pe săptămână. În afara acestor ore, la cerere, ofertantul este obligat să se prezinte în maxim 30 de minute.

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.



- f. La DADPP, CNIPT, Castelul Banffy și DAESA se va face deplasarea doar la cerere. La CZPC se va face o revizie trimestrială
- e. Ofertantul va prezenta declarație de disponibilitate pentru 4 persoane: 3 desemnate la sediul CJ Cluj din Calea Dorobanților nr. 106 și 1 persoană care să le înlocuiască la nevoie.

### 3.2 Autoritatea/entitatea contractantă are următoarele obligații principale:

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

### 3.3 Oferta financiară trebuie să conțină obligatoriu:

- a. oferta financiară pentru mentenanța echipamentelor specificate la punctul 2.1.1.
- b. oferta financiară pentru 340 conturi Microsoft 365 din care 24 au servicii în plus față de Business Standard conturi de utilizatori Microsoft 365 pentru 12 luni conform punctului 2.1.2;
- c. oferta financiară defalcată pe echipamente, licențe, licențe pentru servicii de securitate, piese de schimb și accesorii conform punctului 2.1.3, detaliate în Anexa 1.
- d. mentenanța și administrarea echipamentelor din sala de ședință conform punctului 2.1.4
- e. mentenanța și administrarea echipamentelor de telefonie IP conform punctului 2.1.5

În temeiul Regulamentului (UE) nr. 2016/679 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 (Regulamentul general privind protecția datelor) și al Legii nr. 190/2018 Consiliul Județean Cluj prelucrează date cu caracter personal, cu asigurarea securității și confidențialității acestora.



Oferta pentru activitatea de mentenanță se va calcula adunând tarifele lunare pentru cele 8 luni.

Prețul final al ofertei va rezulta din suma dintre prețul pentru activitatea de mentenanță, pretul aferent abonamentului pentru 340 conturi de utilizatori Microsoft 365 pentru un an de zile și prețul total al echipamentelor/subansamblelor din Anexa 1.

Prețurile din Anexa 1 se vor păstra pe tot parcursul contractului. Toate manoperele de instalare/înlocuire / configurare trebuie să fie incluse.

Oferta va fi exprimată în lei.

#### 4. Modalități și condiții de plată

Plata se va efectua lunar în lei prin Trezoreria Cluj Napoca în termen de 30 de zile de la emiterea facturii de către furnizor.

Întocmit,

