# KOMPIUTERINIO TINKLO PRIEŽIŪROS PASLAUGOS TEIKIMO TAISYKLĖS

## 1. Paslaugos apibrėžimas

1.1. Kompiuterinio tinklo priežiūros paslauga skirta užtikrinti Kliento lokaliojo (LAN), belaidžio (Wi-Fi) ir išorinio (WAN) tinklo infrastruktūros stabilų veikimą, prieinamumą ir bazinį saugumą. Paslauga apima tinklo įrangos administravimą, stebėseną, konfigūracijų palaikymą ir veikimo optimizavimą, trikdžių diagnostiką ir šalinimą, programinės įrangos atnaujinimus, tinklo segmentavimą, saugumo politikų valdymą. Tikslas – užtikrinti nenutrūkstamą duomenų perdavimą tarp įrenginių, saugią prieigą prie išteklių ir stabilią įmonės veiklą.

1.2. Ši paslauga apima tik šiame dokumente aiškiai nurodytas funkcijas ir negali būti interpretuojama kaip pilnas IT infrastruktūros administravimas, saugumo valdymas ar sistemų palaikymas, jei tai nėra aiškiai numatyta atskiroje sutartyje.

## 2. Paslaugos apimtis

2.1. LAN infrastruktūra

- 2.1.1. Maršrutizatorių (vidinių / perimetrinių) konfigūravimas ir priežiūra – srauto valdymas tarp vietinių tinklų ir išorinio WAN.
- 2.1.2. Jungiklių (switch) administravimas.
- 2.1.3. – Valdomi jungikliai (Managed) – VLAN konfigūracija, QoS, stebėsena.
- 2.1.4. – PoE jungikliai – IP telefonų, belaidžių prieigos taškų, vaizdo kamerų maitinimas.
- 2.1.5. – L3 jungikliai – maršrutizavimo ir perjungimo (routing / switching) funkcijų valdymas.
- 2.1.6. Patch panelių priežiūra ir struktūrizuoto kabeliavimo dokumentavimas.
- 2.1.7. Media konverterių (fiber–copper) priežiūra.
- 2.1.8. Tinklo plokščių (NIC) konfigūracija ir tvarkyklių priežiūra darbo vietose ir serveriuose.

2.2. WAN ir perimetro saugumas

- 2.2.1. Ugniasienės (firewalls): tradicinės ir naujos kartos (NGFW) su IDS/IPS, SSL inspekcija, aplikacijų kontrolė.
- 2.2.2. IDS/IPS – įsilaužimų aptikimo / prevencijos sistemų diegimas ir stebėjimas.
- 2.2.3. SD-WAN – kelių ryšio linijų valdymas ir srauto optimizavimas.
- 2.2.4. Apkrovos balansavimo (Load balancer) sprendimų palaikymas – apkrovos paskirstymas tarp paslaugų ar serverių.
- 2.2.5. WAN optimizavimo sprendimų priežiūra – greitaveikos didinimas tarp nutolusių padalinių.

2.3. Belaidė infrastruktūra (WiFi)

- 2.3.1. Prieigos taškų (Access Points) konfigūravimas ir administravimas: vietinių, valdomų valdikliu (controller-based) ar debesijos (Meraki, UniFi) sprendimų palaikymas.
- 2.3.2. Belaidžių valdiklių (Wireless Controllers) administravimas.
- 2.3.3. Lauko (outdoor) belaidžių tiltų konfigūravimas (P2P, PtMP).
- 2.3.4. Svečių Wi-Fi vartų (Guest Gateways) diegimas ir segmentuotas srauto atskyrimas.

2.4. Nuotolinė ir saugi prieiga

- 2.4.1. VPN sprendimų administravimas (Site-to-Site VPN, Client VPN, SSL, IPsec).
- 2.4.2. ZTNA (Zero Trust Network Access) sprendimų palaikymas.
- 2.4.3. MFA integracija – dviejų ar daugiau faktorių autentifikacijos palaikymas nuotoliniams vartotojams.

2.5. Palaikymo ir priežiūros darbai

- 2.5.1. Įrangos ir konfigūracijų atnaujinimas (firmware, OS).
- 2.5.2. Trikčių šalinimas, veikimo testavimas ir optimizavimas.
- 2.5.3. Tinklo našumo (QoS, srauto apkrovos) analizė ir tobulinimas.
- 2.5.4. Reguliarus konfigūracijų atsarginių kopijų darymas (jei techniškai įmanoma).
- 2.5.5. Vendor'ių (gamintojų) palaikymo koordinavimas.
- 2.5.6. Tinklo dokumentacijos ir topologijos atnaujinimas.
- 2.5.7. Periodinės ataskaitos apie tinklo būklę, incidentus ir atliktus darbus.

## 3. Paslaugos ribos

3.1. Paslauga teikiama naudojant standartizuotus įrankius ir metodus.
3.2. Palaikomi tik įrangos (Assets) sutarties priede įtraukti tinklo įrenginiai.
3.3. Individualūs sprendimai as nestandartinės architektūros palaikomos tik papildomai susitarus.
3.4. „Heksimus“ neprivalo palaikyti nestandartinių ar nepalaikomų gamintojų sprendimų.
3.5. Paslauga neapima naujos įrangos tiekimo ar fizinio diegimo darbų (nebent užsakyta atskirai).
3.6. Neapima tinklo kabeliavimo, montavimo darbų (nebent užsakyta atskirai).
3.7. Neapima trečiųjų šalių ryšio tiekėjų (ISP) ar debesijos paslaugų trikdžių sprendimo.
3.8. Neapima nestandartinių aplikacijų ar sistemų, kurios nėra įtrauktos į tinklo paslaugos valdymo sąrašą.
3.9. Neapima pilno IT saugumo valdymo (SOC, SIEM, Pentest, įsilaužimų simuliacijos, saugumo auditas, atitikties vertinimas), jei tai nėra užsakyta atskirai.
3.10. Neapima nuolatinės 24/7 tinklo stebėsenos (nebent užsakyta atskirai).
3.11. Klientas atsako už licencijuotos įrangos, programinės įrangos ir ryšio sutarčių galiojimą.
3.12. „Heximus“ neprisiima atsakomybės už tinklo trikdžius, kilusius dėl kliento atliktų pakeitimų be suderinimo.
3.13. „Heximus“ neatsako už duomenų praradimą, jei Klientas neturi tinkamai veikiančios atsarginių kopijų infrastruktūros.
3.14. Visi darbai, nepatenkantys į šios paslaugos apimtį vykdomi tik pagal atskirą užsakymą, apmokestinami papildomai ir derinami individualiai.

## 4. Atsakomybės ir sąlygos

4.1. Kliento atsakomybės
  4.1.1. Pateikti tikslią informaciją apie tinklo infrastruktūrą.
  4.1.2. Užtikrinti licencijų ir sutarčių galiojimą.
  4.1.3. Nekeisti konfigūracijų be suderinimo.
  4.1.4. Užtikrinti atsarginių kopijų egzistavimą.
4.2. „Heksimus“ atsakomybės
  4.2.1. Vykdyti tik šioje paslaugoje apibrėžtas funkcijas.
  4.2.2. Užtikrinti administracinius ir konfigūracinius veiksmus.
  4.2.3. Teikti rekomendacijas pagal turimus duomenis.
4.3. Atsakomybės ribojimas
  4.3.1. „Heksimus“ neatsako už:
    - Trečiųjų šalių (ISP, cloud, vendor) veikimą.
    - Tinklo sutrikimus dėl išorinių veiksnių ar gamintojų klaidų.
    - Klientui atliktus nesuderintus veiksmus.
    - Nepalaikomos ar nestandartinės įrangos veikimą
4.4. Finansinė ir rizikos atsakomybė
  4.4.1. „Heksimus“ neatsako už:
    - Tiesioginius ar netiesioginius nuostolius.
    - Negautas pajamas.
    - Tinklo prastovas dėl išorinių veiksnių.
    - Saugumo incidentus, jei tai nėra atskira paslauga.
4.5. Konfigūracijų ir duomenų saugumas
  4.5.1. Atsarginės konfigūracijų kopijos yra Kliento atsakomybė
  4.5.2. „Heksimus“ nebūtinai vykdo atsarginių kopijų atstatymo tikrinimą.
  4.5.3. Atkūrimo testai nėra įtraukti (nebent sutarta atskirai)
4.6. Priklausomybės nuo trečiųjų šalių
  4.6.1. Paslauga priklauso nuo:
    - Interneto tiekėjų.
    - Įrangos gamintojų.
    - Debesijos platformų.
  4.6.2. Funkcionalumas gali keistis nepriklausomai nuo „Heksimus“.

## 5. Paslaugos teikimo režimas

5.1. Paslaugos teikimo režimas nurodytas „BENDROSIOS PASLAUGŲ TEIKIMO SĄLYGOS“ 1.3 ir 7.5 punktuose.
5.2. Žodiniai ar neformalūs prašymai nelaikomi galiojančiais.
5.3. „Heksimus“ turi teisę atmesti užklausą, jei ji:
- Viršija paslaugos apimtį.
- Prieštarauja gerosioms praktikoms.
- Kelia saugumo ar teisinę riziką.

5.4. Nuotolinė pagalba teikiama kaip prioritetinis problemų sprendimo būdas; atvykimas į vietą organizuojamas, jei problema neišsprendžiama nuotoliniu būdu.
5.5. Ne darbo metu incidentai sprendžiami pagal atskirą susitarimą ar papildomą paslaugų paketą.

## 6. Incidentų eskalacijos lygiai

6.1. 1 lygio pagalba (L1): pirmo kontakto pagalba – baziniai tinklo patikrinimai, vartotojų VPN nustatymai, paprasti maršrutizatoriaus ar jungiklio konfigūracijos klausimai.
6.2. 2 lygio pagalba (L2): sudėtingesnės problemos – VLAN segmentacija, ugniasienės taisyklių diagnostika, WAN srautų analizė, belaidžių įrenginių trikdžiai.
6.3. 3 lygio pagalba (L3): eskalacija į gamintoją ar specializuotus inžinierius – aparatinės įrangos defektai, licencijavimo problemos, integruotų SD-WAN ar NGFW sprendimų klaidos.
6.4. Incidentų eskalacija vykdoma pagal nustatytą tvarką – jei problema neišsprendžiama L1 lygyje per nustatytą laiką, ji perkeliama į L2, o prireikus – į L3.
6.5. Sprendimo laikas priklauso nuo gamintojo ir infrastruktūros.
6.6. Klientas informuojamas apie eskalacijos eigą, numatomą sprendimo laiką ir galimus veiklos apribojimus.

## 7. Paslaugos interpretavimo taisyklė

7.1. Paslauga interpretuojama tik pagal šiame dokumente nurodytą apimtį.
7.2. Bet koks platesnis interpretavimas laikomas negaliojančiu.
7.3. Visi papildomi lūkesčiai turi būti formalizuoti.