3. Kompiuterinio tinklo priežiūros paslaugos teikimo taisyklės

3.1 Paslaugos apibrėžimas

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

3.2 Paslaugos apimtis

LAN infrastruktūra

- Maršrutizatorių (vidinių / perimetrinių) konfigūravimas ir priežiūra – srauto valdymas tarp vietinių tinklų ir išorinio WAN.
- Jungiklių (switch) administravimas:
- – Valdomi jungikliai (Managed) – VLAN konfigūracija, QoS, stebėsena.
- – PoE jungikliai – IP telefonų, belaidžių prieigos taškų, vaizdo kamerų maitinimas.
- – L3 jungikliai – maršrutizavimo ir perjungimo funkcijų valdymas.
- Patch panelių priežiūra ir struktūrizuoto kabeliavimo dokumentavimas.
- Media konverterių (fiber–copper) priežiūra.

Tinklo plokščių (NIC) konfigūracija ir tvarkyklių priežiūra darbo vietose ir serveriuose.

WAN ir perimetro saugumas

- Ugniasienės (firewalls): tradicinės ir naujos kartos (NGFW) su IDS/IPS, SSL inspekcija, aplikacijų kontrole.
- IDS/IPS – įsilaužimų aptikimo / prevencijos sistemų diegimas ir stebėjimas.
- SD-WAN – kelių ryšio linijų valdymas ir srauto optimizavimas.
- Load balancer'iai – apkrovos paskirstymas tarp paslaugų ar serverių (F5, Kemp, HAProxy ir kt.).
- WAN optimizatoriai – greitaveikos didinimas tarp nutolusių padalinių.

Belaidė infrastruktūra (WiFi)

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

Nuotolinė ir saugi prieiga

- VPN sprendimų administravimas (Site-to-Site, Client, SSL, IPsec).
- ZTNA (Zero Trust Network Access) vartų priežiūra ir prieigos politikų taikymas.
- MFA integracija – dviejų ar daugiau faktorių autentifikacijos palaikymas nuotoliniams vartotojams.

Palaikymo ir priežiūros darbai

- Įrangos ir konfigūracijų atnaujinimas (firmware, OS).
- Trikčių šalinimas, veikimo testavimas ir optimizavimas.

- Tinklo našumo (QoS, srauto apkrovos) analizė ir tobulinimas.
- Reguliarus konfigūracijų atsarginių kopijų darymas.
- Vendorų (gamintojų) palaikymo koordinavimas.
- Tinklo dokumentacijos ir topologijos atnaujinimas.
- Periodinės ataskaitos apie tinklo būklę, incidentus ir atliktus darbus.

3.3 Paslaugos ribos

- Paslauga neapima naujos įrangos tiekimo ar fizinio diegimo darbų (nebent užsakyta atskirai).
- Neapima trečiųjų šalių ryšio tiekėjų (ISP) ar debesijos paslaugų trikčių sprendimo.
- Neapima nestandartinių aplikacijų ar sistemų, kurios nėra įtrauktos į tinklo paslaugos valdymo sąrašą.
- Klientas atsako už licencijuotos įrangos, programinės įrangos ir ryšio sutarčių galiojimą.
- „Heximus“ neprisiima atsakomybės už tinklo trikdžius, kilusius dėl kliento atliktų pakeitimų be suderinimo.
- Neapima saugumo testavimo, įsilaužimų simuliacijų ar audito, jei tai nėra užsakyta atskirai.
- „Heximus“ neatsako už duomenų praradimą, jei Klientas neturi tinkamai veikiančios atsarginių kopijų infrastruktūros.

3.4 Paslaugos teikimo režimas

- Paslauga teikiama darbo dienomis nuo 8:00 iki 18:00 (išskyrus valstybines šventes).
- Užklausos priimamos el. paštu, telefonu arba per pagalbos sistemą (servicedesk).
- Reagavimo laikas priklauso nuo incidento kritiškumo:
    - Kritinis incidentas (Nutrūkęs ryšys, neveikia LAN/WAN jungtis, paveikti verslo procesai) – reagavimas pradėtas per 1 val.
    - Vidutinio lygio incidentas (dalinis ryšio sutrikimas, degradavęs veikimas) – reagavimas per 4 val.
    - Mažos svarbos užklausa (optimizacijos, patarimai, smulkūs nustatymai) – reagavimas per 1 darbo dieną.
- Nuotolinė pagalba teikiama kaip prioritetinis problemų sprendimo būdas; atvykimas į vietą organizuojamas, jei problema neišsprendžiama nuotoliniu būdu.
- Ne darbo metu incidentai sprendžiami pagal atskirą susitarimą ar papildomą paslaugų paketą.

3.5 Atsarginės kopijos ir tinklo konfigūracijų saugumas

- Klientas turi užtikrinti, kad tinklo įrangos konfigūracijos būtų reguliariai kopijuojamos į centrinę sistemą.
- „Heximus“ rekomenduoja naudoti centralizuotą konfigūracijų valdymo sprendimą (pvz., RANCID, NetBox, Zabbix Backup, ar debesijos kopijų paslaugą).
- Atsarginių kopijų testavimas ir atkūrimo planų patikra – Kliento atsakomybė, nebent užsakyta papildoma paslauga.
- „Heximus“ neatsako už konfigūracijų ar duomenų praradimą, jei nėra patikimos atsarginių kopijų sistemos.

Rekomenduojama naudoti prieigos valdymą pagal roles (RBAC), slaptažodžių politiką ir MFA, tinklo įrangos OS atnaujinimus, ugniasienės politikų periodinį peržiūrėjimą.

3.6 Incidentų eskalacijos lygiai

- 1 lygio pagalba (L1): pirmo kontakto pagalba – baziniai tinklo patikrinimai, vartotojų VPN nustatymai, paprasti maršrutizatoriaus ar jungiklio konfigūracijos klausimai.
- 2 lygio pagalba (L2): sudėtingesnės problemos – VLAN segmentacija, ugniasienės taisyklių diagnostika, WAN srautų analizė, belaidžių įrenginių trikdžiai.
- 3 lygio pagalba (L3): eskalacija į gamintoją ar specializuotus inžinierius – aparatinės įrangos defektai, licencijavimo problemos, integruotų SD-WAN ar NGFW sprendimų klaidos.

- Incidentų eskalacija vykdoma pagal nustatytą tvarką: jei problema neišsprendžiama L1 lygyje per nustatytą laiką, ji perkeliama į L2, o prireikus – į L3.
- Klientas informuojamas apie eskalacijos eigą, numatomą sprendimo laiką ir galimus veiklos apribojimus.