1. Serverių priežiūros paslaugos teikimo taisyklės

1.1 Paslaugos apibrėžimas

Serverių priežiūros paslauga skirta užtikrinti Kliento serverių, virtualizacijos aplinkų, operacinių sistemų, paslaugų (angl. services) bei duomenų bazių stabilų veikimą, saugumą ir atnaujinimus. Paslauga apima sistemų monitoringą, trikdžių diagnostiką ir šalinimą, našumo bei saugumo palaikymą, duomenų apsaugą ir rekomendacijų teikimą.

1.2 Paslaugos apimtis

- Serverių administravimas: vartotojų ir paslaugų paskyrų valdymas, teisių priskyrimas, domeno ir katalogo paslaugų priežiūra.
- Operacinių sistemų priežiūra: serverinių OS diegimas, atnaujinimų ir saugumo pataisų įdiegimas, stabilumo ir suderinamumo užtikrinimas.
- Programinės įrangos ir paslaugų priežiūra: verslo aplikacijų, duomenų bazių (pvz., MS SQL, MySQL, PostgreSQL), failų (file server) ir spausdinimo (print server) paslaugų, el. pašto serverių, web serverių administravimas.
- Virtualizacijos platformų priežiūra: Proxmox, VMware, Hyper-V ar kitų virtualizacijos aplinkų administravimas, resursų paskirstymas, VM kūrimas ir optimizavimas.
- Saugumo priežiūra: ugniasienių konfigūravimas, prieigos kontrolė, daugiafaktorė autentifikacija, pažeidžiamumų analizė, audito žurnalų stebėsena.
- Tinklo paslaugų priežiūra serveryje: DNS, DHCP, VPN, katalogo paslaugų (AD/LDAP) veikimo palaikymas.
- Monitoringas: 24/7 stebėsena dėl resursų apkrovos (CPU, RAM, diskų, tinklo), paslaugų veikimo, saugumo įvykių.
- Ataskaitos: serverių būklės, resursų naudojimo, incidentų ir atliktų darbų periodinis pateikimas.
- Dokumentacijos tvarkymas: serverių, konfigūracijų ir paslaugų dokumentacijos atnaujinimas pagal susitarimą.

1.3 Paslaugos ribos

- Neapima specifinių ar nestandartinių trečiųjų šalių verslo aplikacijų palaikymo (nebent susitarta atskirai).
- Neapima duomenų atkūrimo iš sugadintų laikmenų (nebent užsakyta atskira paslauga).
- Neapima naujų serverių ar tinklo įrangos tiekimo, garantinio/pogarantinio remonto – už tai atsako įrangos gamintojas ar tiekėjas.
- Klientas atsako už programinės įrangos licencijų įsigijimą ir teisėtą naudojimą.
- Kliento atlikti pakeitimai be „Heximus“ suderinimo gali sukelti trikdžius, už kuriuos „Heximus“ neprisiima atsakomybės.
- „Heximus“ neatsako už trečiųjų šalių (pvz., interneto paslaugų, debesijos paslaugų) sukeltus trikdžius.
- Neapima darbuotojų mokymų ar detalių konsultacijų – nebent susitarta atskirai.
- „ Heximus“ neatsako už Kliento serverių duomenų saugumą, jei nėra naudojama tinkama atsarginių kopijų sistema ar papildomi saugumo sprendimai.

1.4 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 (serveris visiškai neveikia, sustoja esminės paslaugos) – reagavimas pradėtas per 1 val.
    - Vidutinio lygio incidentas (ribotas paslaugų veikimas, bet yra alternatyvų) – 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.

1.5 Atsarginės kopijos ir duomenų saugumas

- Klientas privalo užtikrinti, kad svarbūs duomenys būtų reguliariai kopijuojami į centrinę atsarginių kopijų sistemą ar debesiją.
- „Heximus“ rekomenduoja naudoti centralizuotą, automatizuotą atsarginių kopijų sprendimą su periodiniais testiniais atkūrimais.
- Atsarginių kopijų testavimas yra Kliento atsakomybė, nebent užsakoma papildoma paslauga.
- „Heximus“ neatsako už duomenų praradimą, jei Klientas neturi patikimos atsarginių kopijų sistemos.
- Rekomenduojama naudoti papildomas saugumo priemones: duomenų šifravimą, prieigos teisių segmentavimą (PAM), SIEM sprendimus, daugiafaktorę autentifikaciją.
- Saugumo incidentų atveju „Heximus“ gali padėti atlikti analizę ir pateikti rekomendacijas, tačiau galutinis duomenų saugumo užtikrinimas yra Kliento atsakomybė.

1.6 Incidentų eskalacijos lygiai

- 1 lygio pagalba (L1) – pagrindinės serverių priežiūros užduotys: paslaugų stebėsena, paprasti nustatymai, vartotojų paskyrų valdymas, bazinė diagnostika.
- 2 lygio pagalba (L2) – sudėtingesnės problemos: operacinių sistemų trikdžiai, duomenų bazių ar paslaugų veikimo sutrikimai, virtualizacijos platformų diagnostika.
- 3 lygio pagalba (L3) – eskalacija gamintojui ar specializuotiems inžinieriams: aparatinės įrangos defektai, specifinių sistemų ar trečiųjų šalių sprendimų klaidos.
- 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 ir planuojamą sprendimo laiką.