1. Kompiuterinių darbo vietų priežiūros paslaugos teikimo taisyklės

1.1 Paslaugos apibrėžimas

Kompiuterinių darbo vietų (KDV) priežiūros paslauga skirta užtikrinti Kliento naudotojų darbo kompiuterių, operacinių sistemų, biuro programų, periferinės įrangos bei ryšio priemonių stabilų veikimą, atnaujinimus ir apsaugą. Paslauga apima kasdienės pagalbos suteikimą vartotojams, trikdžių diagnostiką ir šalinimą, darbo našumo ir saugumo palaikymą.

1.2 Paslaugos apimtis

- Darbo vietų administravimas: vartotojų profilių kūrimas, nustatymų konfigūravimas, kompiuterių pridėjimas prie domeno ar darbo grupės, naudotojų teisių valdymas.
- Operacinių sistemų priežiūra: OS diegimas / perinstaliavimas, atnaujinimų įdiegimas, veikimo stabilumo užtikrinimas.
- Programinės įrangos priežiūra: standartinių biuro, komunikacijos, saugumo programų diegimas, konfigūravimas, atnaujinimas.
- Saugumo priežiūra: antivirusinės apsaugos diegimas ir atnaujinimas, ugniasienės ir saugumo politikų taikymas, naudotojų slaptažodžių politikos įgyvendinimas.
- Įrangos palaikymas: spausdintuvų, skenerių, monitorių ir kitos periferijos prijungimas bei nustatymas.
- Tinklo paslaugų priežiūra darbo vietoje: prieigos prie interneto, vietinio tinklo, VPN nustatymas ir trikčių šalinimas.
- Nuotolinė pagalba: vartotojų konsultavimas ir problemų sprendimas nuotoliniu būdu.
- Ataskaitos: darbo vietų būklės, naudotojų incidentų ir atliktų darbų periodinis pateikimas.
- Dokumentacijos atnaujinimas: įrangos ir vartotojų darbo vietų dokumentacijos tvarkymas pagal susitarimą.

1.3 Paslaugos ribos

- Neapima nestandartinės ar specifinės verslo programinės įrangos diegimo ir palaikymo (nebent susitarta atskirai).
- Neapima duomenų atkūrimo iš pažeistų diskų ar atsarginių kopijų sistemų administravimo (nebent užsakyta atskirai).
- Neapima naujų kompiuterių, serverių ar tinklo įrangos tiekimo, garantinio / pogarantinio remonto – už tai atsako įrangos gamintojas ar tiekėjas.
- Klientas atsako už licencijuotos programinės įrangos įsigijimą, licencijų galiojimą bei laikymąsi teisinių reikalavimų.
- Kliento atlikti pakeitimai be „Heximus“ suderinimo gali sąlygoti trikdžius, už kuriuos „Heximus“ neprisiima atsakomybės.
- „Heximus“ neatsako už trečiųjų šalių teikiamų paslaugų ar tiekėjų (pvz., interneto paslaugų tiekėjo, debesijos paslaugų) trikdžius.
- Neapima darbuotojų mokymų ar išsamių naudotojų instruktavimų – nebent susitarta atskirai.
- „Heximus“ neprisiima atsakomybės už Kliento darbo vietų duomenų saugumą, jei Klientas neturi tinkamos atsarginių kopijų sistemos ar papildomų saugumo sprendimų.

1.4 Paslaugos teikimo režimas

- Paslauga teikiama darbo dienomis nuo 8:00 iki 18:00 (išskyrus valstybines šventes).
- Užklausos priimamos:
    - el. paštu pagalba@heximus.lt
    - per pagalbos sistemą msp.heximus.lt
    - telefonu 052137307, bet tik tais atvejais kai pateikti užklausą kitais būdais nėra.
- Reagavimo laikas priklauso nuo incidento kritiškumo:
    - Kritinis incidentas (darbo vieta visiškai neveikia, sustoja esminiai procesai) – reagavimas pradėtas per 2 val.
    - Vidutinio lygio incidentas (ribotas darbo funkcionalumas, bet yra alternatyvų) – reagavimas per 4 val.

- Mažos svarbos užklausa (klausimai, konsultacijos, smulkūs nustatymai) – reagavimas per 1 darbo dieną.

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

1.5 Atsarginės kopijos ir duomenų saugumas

- Klientas privalo užtikrinti, kad darbo vietose saugomi svarbūs duomenys būtų reguliariai kopijuojami į centrinę atsarginių kopijų sistemą ar debesijos paslaugą.
- „Heximus“ rekomenduoja naudoti centralizuotą atsarginių kopijų sprendimą (pvz., serverinę ar debesijos atsarginių kopijų sistemą), o ne tik lokalų saugojimą darbo vietoje.
- Atsarginių kopijų patikimumo testavimas yra Kliento atsakomybė, nebent užsakoma papildoma paslauga.
- „Heximus“ neatsako už duomenų praradimą ar sugadinimą, jei Klientas neturi tinkamai veikiančios atsarginių kopijų sistemos.
- Rekomenduojama naudoti papildomus saugumo sprendimus: disko šifravimą, daugiafaktorę autentifikaciją, reguliarią antivirusinės apsaugos atnaujinimų kontrolę.
- Saugumo incidentų atveju „Heximus“ gali padėti diagnozuoti problemą ir pateikti rekomendacijas, tačiau galutinis duomenų saugumo užtikrinimas yra Kliento atsakomybė.

1.6 Incidentų eskalacijos lygiai

- 1 lygio pagalba (L1) – pirmo kontakto pagalba: vartotojų klausimai, paprasti nustatymai, slaptažodžių atstatymai, bazinės trikčių diagnostikos užduotys.
- 2 lygio pagalba (L2) – sudėtingesnės problemos, reikalaujančios gilesnės analizės: OS trikdžiai, programinės įrangos klaidų šalinimas, tinklo konfigūracijos klausimai.
- 3 lygio pagalba (L3) – eskalacija į gamintoją ar specializuotus inžinierius: nestandartinės problemos, aparatinės įrangos defektai, trečiųjų šalių 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 ir numatomą sprendimo laiką.