

4. Microsoft 365 vartotojų priežiūros paslaugos teikimo taisyklės

4.1 Paslaugos apibrėžimas

Microsoft 365 vartotojų priežiūros paslauga (Exchange, Teams, OneDrive, SharePoint ir kt.) skirta M365 aplinkos ir jos vartotojų administravimui, prieigos kontrolei, licencijų ir resursų optimizavimui, sprendimų diegimui ir palaikymui.

4.2 Paslaugos apimtis

- Vartotojų administravimas: kūrimas, šalinimas, teisių keitimas, slaptažodžių atstatymas, bendrinių dėžučių, grupių valdymas, licencijų priskyrimas/nuėmimas.
- El. pašto administravimas: pašto dėžučių konfigūravimas, slapyvardžių ir peradresavimų nustatymai, politikų keitimas.
- Saugumo priežiūra: prisijungimų stebėseną, daugiafaktoriškos autentifikacijos (MFA) valdymas, slaptažodžių politikos įgyvendinimas, saugos įspėjimų analizė ir eskalavimas, prisijungimų ir audito ataskaitų analizė.
- Teams ir OneDrive palaikymas: komandos, svečių prieigos nustatymai, failų bendrinimo ir prieigos kontrolė.
- SharePoint priežiūra: vartotojų prieigos suteikimas / atėmimas, bendrinimo nustatymų tvarkymas.
- Problemų diagnostika ir sprendimas, naudotojų konsultavimas.
- Licencijų ir vartotojų ataskaitų pateikimas.
- Vartotojų ir prieigos teisių dokumentacijos atnaujinimas (pagal susitarimą).

4.3 Paslaugos ribos

- Neapima duomenų migracijų, automatizacijų, hibridinės aplinkos diegimo, Intune diegimo, DLP konfigūracijos ar saugumo didinimo, sharepoint intraneto kūrimo ar kitų sudėtingų konfigūracijų, nebent užsakyta atskirai.
- Neapima trečiųjų šalių integracijų ar papildinių palaikymo.
- Klientas atsako už licencijų aktyvumą, paskirtį ir laiku atliktą apmokėjimą.
- Kliento atlikti pakeitimai be „Heximus“ suderinimo gali sąlygoti trikdžius, už kuriuos „Heximus“ neprisiima atsakomybės.
- „Heximus“ neatsako už Microsoft 365 debesijos trikdžius ar incidentus, atsirandančius pačioje Microsoft infrastruktūroje (pvz., „Outlook“ neveikimas globaliai).
- Neapima mokymų ar vartotojų apmokymo – nebent susitarta atskirai.
- „Heximus“ neprisiima atsakomybės už Kliento Microsoft 365 aplinkos ar vartotojų paskyrų saugumą nuo išorinių ar vidinių atakų, duomenų nutekėjimo, neteisėtų prisijungimų ar kitų kibernetinių incidentų.