HX Paslaugų aprašymas.

Redakcija V4.2. Galioja nuo paskelbimo Paslaugos Vykdytojo interneto svetainėje www.heximus.lt dienos. Jau sudarytiems Paslaugų užsakymams pakeitimai taikomi Bendrosios dalies 3.2.5 punkte nustatyta tvarka.

Šis dokumentas yra Bendrųjų paslaugų teikimo sąlygų (Bendrosios dalies) priedas – Paslaugų teikimo taisyklės. Jame vartojamos sąvokos turi Bendrosios dalies 1 skyriuje nustatytą reikšmę. Esant prieštaravimams tarp šio dokumento ir Bendrosios dalies, taikoma Bendroji dalis.

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 ataskaitos teikiamos pagal susitarimą arba Kliento prašymu.
- 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 Paslaugos Vykdytojo suderinimo gali sąlygoti trikdžius, už kuriuos Paslaugos Vykdytojas neprisiima atsakomybės.

- Paslaugos Vykdytojas 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.
- Neapima informacijos saugumo stebėsenos (SOC), pažeidžiamumų vertinimo, saugumo žurnalų ar prisijungimų analizės, įsilaužimų testavimo ir saugumo incidentų tyrimo – tokios paslaugos teikiamos tik pagal atskirą užsakymą ir atskirą paslaugos aprašymą.
- Paslaugos Vykdytojas 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 poilsio ir švenčių dienas).
- Užklausos priimamos:
    - el. paštu pagalba@heximus.lt
    - per pagalbos sistemą msp.heximus.lt
    - telefonu +370 5 213 7307, kai nėra galimybės pateikti Užklausos kitais Informavimo kanalais.
- Reakcijos ir Sprendimo laikai nustatomi pagal Kliento Paslaugų užsakyme pasirinktą SLA planą (Bendrosios dalies 7.5 punktas). Jeigu SLA planas nepasirinktas, taikomi šie orientaciniai reakcijos laikai:
    - 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 taikomi Bendrosios dalies 7.5 punkte nurodyti reagavimo terminai. Gedimai ne darbo metu šalinami tik tuo atveju, kai budėjimas ne darbo metu nurodytas Paslaugų užsakyme ar sutartas atskirai.

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.
- Paslaugos Vykdytojas 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.
- Paslaugos Vykdytojas neatsako už duomenų praradimą ar sugadinimą, jei Klientas neturi tinkamai veikiančios atsarginių kopijų sistemos; ši nuostata netaikoma tiek, kiek duomenų praradimą ar sugadinimą lėmė Paslaugos Vykdytojo kaltė (Bendrosios dalies 8 skyrius).
- Rekomenduojama naudoti papildomus saugumo sprendimus: disko šifravimą, daugiafaktorę autentifikaciją, reguliarią antivirusinės apsaugos atnaujinimų kontrolę.

- Saugumo incidentų atveju Paslaugos Vykdytojas 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.

2. Serverių priežiūros paslaugos teikimo taisyklės

2.1 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.

2.2 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, daugiafaktorės autentifikacijos administravimas, gamintojų saugos pataisų diegimas.
- Tinklo paslaugų priežiūra serveryje: DNS, DHCP, VPN, katalogo paslaugų (AD/LDAP) veikimo palaikymas.
- Monitoringas: 24/7 automatinė stebėsena (reagavimas – pagal pasirinktą SLA planą) dėl resursų apkrovos (CPU, RAM, diskų, tinklo) ir paslaugų veikimo.
- Ataskaitos: serverių būklės, resursų naudojimo, incidentų ir atliktų darbų ataskaitos teikiamos pagal susitarimą arba Kliento prašymu.
- Dokumentacijos tvarkymas: serverių, konfigūracijų ir paslaugų dokumentacijos atnaujinimas pagal susitarimą.

2.3 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 Paslaugos Vykdytojo suderinimo gali sukelti trikdžius, už kuriuos Paslaugos Vykdytojas neprisiima atsakomybės.
- Paslaugos Vykdytojas neatsako už trečiųjų šalių (pvz., interneto paslaugų, debesijos paslaugų) sukeltus trikdžius.
- Neapima darbuotojų mokymų ar detalių konsultacijų – nebent susitarta atskirai.
- Neapima informacijos saugumo stebėsenos (SOC), pažeidžiamumų vertinimo, saugumo žurnalų ar prisijungimų analizės, įsilaužimų testavimo ir saugumo incidentų tyrimo – tokios paslaugos teikiamos tik pagal atskirą užsakymą ir atskirą paslaugos aprašymą.
- Paslaugos Vykdytojas neatsako už Kliento serverių duomenų saugumą, jei nėra naudojama tinkama atsarginių kopijų sistema ar papildomi saugumo sprendimai.

2.4 Paslaugos teikimo režimas

- Paslauga teikiama darbo dienomis nuo 8:00 iki 18:00 (išskyrus poilsio ir švenčių dienas).
- Užklausos priimamos el. paštu, telefonu arba per pagalbos sistemą (servicedesk).
- Reakcijos ir Sprendimo laikai nustatomi pagal Kliento Paslaugų užsakyme pasirinktą SLA planą (Bendrosios dalies 7.5 punktas). Jeigu SLA planas nepasirinktas, taikomi šie orientaciniai reakcijos laikai:
    - 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 taikomi Bendrosios dalies 7.5 punkte nurodyti reagavimo terminai. Gedimai ne darbo metu šalinami tik tuo atveju, kai budėjimas ne darbo metu nurodytas Paslaugų užsakyme ar sutartas atskirai.

2.5 Atsarginės kopijos ir duomenų saugumas

- Klientas privalo užtikrinti, kad svarbūs duomenys būtų reguliariai kopijuojami į centrinę atsarginių kopijų sistemą ar debesiją.
- Paslaugos Vykdytojas rekomenduoja naudoti centralizuotą, automatizuotą atsarginių kopijų sprendimą su periodiniais testiniais atkūrimais.
- Atsarginių kopijų testavimas yra Kliento atsakomybė, nebent užsakoma papildoma paslauga.
- Paslaugos Vykdytojas neatsako už duomenų praradimą, jei Klientas neturi patikimos atsarginių kopijų sistemos; ši nuostata netaikoma tiek, kiek duomenų praradimą ar sugadinimą lėmė Paslaugos Vykdytojo kaltė (Bendrosios dalies 8 skyrius).
- Rekomenduojama naudoti papildomas saugumo priemones: duomenų šifravimą, prieigos teisių segmentavimą (PAM), SIEM sprendimus, daugiafaktorę autentifikaciją.

- Saugumo incidentų atveju Paslaugos Vykdytojas gali padėti atlikti analizę ir pateikti rekomendacijas, tačiau galutinis duomenų saugumo užtikrinimas yra Kliento atsakomybė.

2.6 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.

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. Paslauga teikiama siekiant palaikyti stabilų tinklo veikimą ir saugią prieigą prie išteklių; konkretūs prieinamumo rodikliai ir jų netaikymo atvejai nustatomi Paslaugų užsakyme ir Bendrosios dalies 7 skyriuje.

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 administravimas.
- 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 parametrų (QoS, srauto prioritetų) konfigūravimas ir trikčių diagnostika.
- Reguliarus konfigūracijų atsarginių kopijų darymas.
- Vendorų (gamintojų) palaikymo koordinavimas.
- Tinklo dokumentacijos ir topologijos atnaujinimas.
- Ataskaitos apie tinklo būklę, incidentus ir atliktus darbus teikiamos pagal susitarimą arba Kliento prašymu.

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.
- Paslaugos Vykdytojas neprisiima atsakomybės už tinklo trikdžius, kilusius dėl kliento atliktų pakeitimų be suderinimo.
- Neapima informacijos saugumo stebėsenos (SOC), pažeidžiamumų vertinimo, saugumo žurnalų analizės, saugumo testavimo, įsilaužimų simuliacijų, audito ir saugumo incidentų tyrimo – tokios paslaugos teikiamos tik pagal atskirą užsakymą ir atskirą paslaugos aprašymą.
- Paslaugos Vykdytojas 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 poilsio ir švenčių dienas).

- Užklausos priimamos el. paštu, telefonu arba per pagalbos sistemą (servicedesk).
- Reakcijos ir Sprendimo laikai nustatomi pagal Kliento Paslaugų užsakyme pasirinktą SLA planą (Bendrosios dalies 7.5 punktas). Jeigu SLA planas nepasirinktas, taikomi šie orientaciniai reakcijos laikai:
  - 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 taikomi Bendrosios dalies 7.5 punkte nurodyti reagavimo terminai. Gedimai ne darbo metu šalinami tik tuo atveju, kai budėjimas ne darbo metu nurodytas Paslaugų užsakyme ar sutartas atskirai.

3.5 Atsarginės kopijos ir tinklo konfigūracijų saugumas

- Klientas turi užtikrinti, kad tinklo įrangos konfigūracijos būtų reguliariai kopijuojamos į centrinę sistemą.
- Paslaugos Vykdytojas 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.
- Paslaugos Vykdytojas neatsako už konfigūracijų ar duomenų praradimą, jei nėra patikimos atsarginių kopijų sistemos; ši nuostata netaikoma tiek, kiek duomenų praradimą ar sugadinimą lėmė Paslaugos Vykdytojo kaltė (Bendrosios dalies 8 skyrius).

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.

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: daugiafaktorės autentifikacijos (MFA) valdymas, slaptažodžių politikos konfigūravimas, standartinių „Microsoft 365“ saugos įspėjimų administravimas ir, Kliento prašymu, standartinių prisijungimų bei naudojimo ataskaitų pateikimas.
- 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 Paslaugos Vykdytojo suderinimo gali sąlygoti trikdžius, už kuriuos Paslaugos Vykdytojas neprisiima atsakomybės.
- Paslaugos Vykdytojas neatsako už Microsoft 365 debesijos trikdžius ar incidentus, atsirandančius pačioje Microsoft infrastruktūroje (pvz., „Outlook“ neveikimas globaliai).
- Neapima mokymų ar vartotojų apmokymo – nebent susitarta atskirai.
- Neapima informacijos saugumo stebėsenos (SOC), pažeidžiamumų vertinimo, saugumo žurnalų ar prisijungimų analizės, įsilaužimų testavimo ir saugumo incidentų tyrimo – tokios paslaugos teikiamos tik pagal atskirą užsakymą ir atskirą paslaugos aprašymą.
- Paslaugos Vykdytojas neprisiima atsakomybės už Kliento Microsoft 365 aplinkos ar vartotojų paskyrų saugumą nuo išorinių ar vidinių atakų, duomenų nutekėjimo, neteisėtų prisijungimų ar kitų kibernetinių incidentų.

5. Microsoft 365 licencijų nuomos paslaugos teikimo taisyklės

5.1 5.1 Paslaugos apibrėžimas

Microsoft 365 licencijų nuomos paslauga leidžia Klientui naudotis Microsoft 365 licencijomis per Paslaugos Vykdytojo CSP partnerystės kanalą, užtikrinant lankstų vartotojų skaičiaus valdymą, skaidrų atsiskaitymą ir kaštų planavimą, centralizuotą licencijų kontrolę bei administravimą.

5.2 Paslaugos apimtis

- Microsoft 365 licencijų registracija, aktyvavimas ir priskyrimas Kliento vartotojams.
- Licencijų kiekio valdymas: pridėjimas, mažinimas, keitimas.
- Pagalba parenkant tinkamiausią licencijų planą.
- Ataskaitų apie licencijų panaudojimą teikimas Kliento prašymu.
- Konsultacijos dėl išlaidų optimizavimo.

5.3 Atsakomybės ir sąlygos

- Klientas atsako už licencijų naudojimą laikantis Microsoft politikos.
- Licencijų mažinimai turi būti inicijuoti iki atsiskaitymo mėnesio pabaigos.
- Licencijos gali būti su 1 mėn. arba 12 mėn. įsipareigojimu (priklausomai nuo plano).
- Paslaugos Vykdytojas neprisiima atsakomybės už Kliento padarytus pakeitimus, jei jie neatitinka licencijavimo politikos.
- Paslauga neapima trečiųjų šalių parduotų ar kitų tiekėjų licencijų administravimo.

6. Mobilių įrenginių valdymo (MDM) paslaugos teikimo taisyklės

6.1 Paslaugos apibrėžimas

Mobilių įrenginių valdymo (MDM) paslauga teikiama „Microsoft Intune“ programinės įrangos pagrindu ir apima:

- pirminį sprendimo diegimą bei konfigūravimą,
- saugumo politikų ir taisyklių kūrimą,
- nuolatinę organizacijoje naudojamų mobilių įrenginių priežiūrą bei administravimą,
- nuotolinį įrenginių valdymą ir ataskaitų teikimą.

6.2 Paslaugos apimtis

- Paslaugos pristatymas,
- Kliento poreikių analizė,

- Įrenginių analizė,
- Licencijų parinkimas ir užsakymas,
- Įrenginių registracijos taisyklių ir politikų kūrimas (Apple, Android, Windows, macOS),
- Autopilot konfigūracija - naujų įrenginių automatizuotam paruošimui,
- Saugumo funkcijų ir politikų nustatymai (diskų šifravimas, PIN/biometrija, „Conditional Access“, įrenginių atitikties politika),
- Operacinės sistemos atnaujinimų politika,
- Standartinių įmonės aplikacijų katalogo sudarymas ir sukonfigūravimas,
- Automatinio aplikacijų atnaujinimo politikos sukūrimas,
- Duomenų apsaugos nustatymų konfigūravimas aplikacijų lygmeniu,
- Wi-Fi ir VPN profilių sukonfigūravimas,
- Įrenginių registracija į „Microsoft Intune“ aplinką,
- Informacijos apie įrenginius ir įdiegtas aplikacijas teikimas,
- Aplikacijų diegimas bei pašalinimas nuotoliniu būdu,
- Prarastų ar pavogtų įrenginių blokavimas, duomenų (pilnas ar dalinis) ištrynimas,
- Ataskaitų iš MDM sistemos teikimas pagal poreikį,
- Naujo įrenginio pridėjimas / seno įrenginio pašalinimas iš sistemos,
- Naudotojų mokymas ir instrukcijų parengimas: prisijungimo prie MDM sistemos, įrenginio aktyvavimo ir veiksmų praradus įrenginį instrukcijos.

6.2.1 Licencijavimas

- Paslaugai veikti būtinos „Microsoft Intune“ licencijos; jos nėra MDM paslaugos dalis, į Paslaugos kainą neįeina ir užsakomos atskirai;
- Klientai, nesinaudojantys šiomis licencijomis, privalo naudoti ar įsigyti tinkamas „Microsoft 365“ arba „Enterprise Mobility + Security“ licencijas (pvz., „Microsoft 365 Business Premium“, E3/E5, EMS E3/E5).

6.2.2 Palaikomos operacinės sistemos

- „Windows 10/11“ – „Pro“, „Education“, „Enterprise“.
- „Android“ – nuo 6.0 versijos.
- „iOS“ – nuo 12.0 versijos.
- „iPadOS“ – nuo 13.0 versijos.
- „macOS“ – nuo 10.13 versijos ir naujesnės.

6.3 Paslaugos ribos

- MDM funkcionalumas priklauso nuo įrenginio gamintojo, modelio ir operacinės sistemos ribojimų,
- Paslaugos Vykdytojas neatsako, jei įrenginių nepavyksta įregistruoti ar pritaikyti politikų dėl netinkamos OS versijos ar kitų techninių kliūčių,
- Jei naudojama programinė įranga neturi palaikymo iš gamintojo arba jis pasibaigęs, Paslaugos Vykdytojas neprisiima atsakomybės už incidentų sprendimą,

- Paslauga neužtikrina automatinės integracijos su kitomis trečiųjų šalių sistemomis, nebent tai iš anksto suderinta atskiru susitarimu. Trečiųjų šalių aplikacijų veikimas nėra garantuojamas.

6.4 Atsakomybės ir sąlygos

Šiame 6.4 punkte nustatytos atsakomybės, ribojimai, sąlygos ir principai taikomi visoms šiame dokumente aprašytoms paslaugoms, nebent konkrečiam paslaugų tipui aiškiai nurodyta kitaip. Esant prieštaravimams tarp šio 6.4 punkto nuostatų ir kitų šio dokumento dalių, taikomos šio 6.4 punkto nuostatos, nebent aiškiai nurodyta kitaip. Esant prieštaravimams tarp šio dokumento ir Bendrosios dalies, taikoma Bendroji dalis.

- Paslaugos Vykdytojas nėra atsakingas už incidentus, kilusius dėl pasenusios ar nelegaliai naudojamos programinės įrangos;
- Paslaugos Vykdytojas neatsako už „Microsoft Intune“, „Azure“ ar kitų debesijos tiekėjų paslaugų trikdžius, nesklandumus ar prieinamumo problemas;
- Paslaugos Vykdytojas negarantuoja skirtingų sistemų, programinės įrangos ar infrastruktūros komponentų suderinamumo, nebent tai aiškiai numatyta atskiru susitarimu;
- Paslaugos Vykdytojas neatsako už netiesioginius nuostolius, įskaitant, bet neapsiribojant, negautas pajamas, veiklos sutrikimus ar reputacinę žalą, nebent imperatyvūs teisės aktai nustato kitaip;
- Klientas privalo nedelsiant pranešti apie prarastus ar pavogtus įrenginius, kitaip Paslaugos Vykdytojas negali užtikrinti laiku atliktų blokavimo/trynimo veiksmų;
- Klientas turi užtikrinti, kad darbuotojai laikytųsi saugumo politikos ir naudotų įrenginius atsakingai;
- Paslaugos Vykdytojas neatsako už duomenų praradimą, sugadinimą ar nutekėjimą, išskyrus tiek, kiek jį lėmė Paslaugos Vykdytojo kaltė; atsakomybės apimtis ir ribos nustatytos Bendrosios dalies 8 skyriuje;
- Klientas atsako už licencijų įsigijimą ir jų galiojimo užtikrinimą;
- Jeigu Paslaugų užsakyme SLA planas nepasirinktas, aukščiau nurodyti reakcijos laikai yra orientaciniai. Pasirinkus SLA planą, taikomi Bendrosios dalies 7 skyriuje nustatyti SLA parametrai, o jų nesilaikymo pasekmes reglamentuoja Bendrosios dalies 7.7 punktas;
- Paslaugos Vykdytojas neteikia specializuotų kibernetinio saugumo paslaugų (saugumo operacijų centro, įsilaužimo testų, incidentų tyrimo ir panašių), nebent tai aiškiai numatyta Paslaugų užsakyme; šiame dokumente nurodyti ugniasienių, prieigų, atnaujinimų ir saugos įvykių administravimo darbai į Paslaugų apimtį įeina. Paslaugos Vykdytojas neatsako už kibernetinius incidentus, neteisėtus prisijungimus, duomenų nutekėjimą ar kitus saugumo pažeidimus, išskyrus Bendrosios dalies 6.13, 7.10.4 ir 8.3.1 punktuose nurodytus atvejus bei Paslaugos Vykdytojo tyčios ar didelio neatsargumo atvejus;
- Paslaugos teikiamos vadovaujantis gerąja IT praktika ir „best efforts“ principu. Klientas supranta ir sutinka, kad paslaugų rezultatai priklauso nuo daugelio

išorinių veiksnių, todėl Paslaugos Vykdytojas negarantuoja konkretaus rezultato ar nepertraukiamo veikimo;

- Paslaugų teikimas priklauso nuo Kliento infrastruktūros, trečiųjų šalių programinės įrangos, paslaugų teikėjų ir gamintojų sprendimų veikimo. Paslaugos Vykdytojas neatsako už sutrikimus, kilusius dėl šių priklausomybių;

- Klientas įsipareigoja:

  – užtikrinti tinkamą IT infrastruktūros būklę;
  – naudoti licencijuotą programinę įrangą;
  – laiku teikti reikalingą informaciją ir prieigas;
  – nedaryti pakeitimų be suderinimo su Paslaugos Vykdytoju.

  Paslaugos Vykdytojas neatsako už paslaugų kokybės ar rezultatų pablogėjimą, jei Klientas nesilaiko šių pareigų;

- Tiek, kiek Paslaugų teikimo metu tvarkomi asmens duomenys, jų tvarkymui taikomos Duomenų tvarkymo taisyklių (DPA) nuostatos, kurios turi viršenybę šio dokumento atžvilgiu;

- Bet kokie papildomi darbai ar paslaugos, nepatenkančios į šiame dokumente apibrėžtą apimtį, laikomi papildomomis paslaugomis ir teikiami tik atskiru Šalių susitarimu, išskyrus atvejus, kai Bendroji dalis ar Duomenų tvarkymo taisyklės nustato kitaip;

- Paslaugų teikimo metu gauta informacija laikoma konfidencialia ir tvarkoma pagal tarp Šalių sudarytą Konfidencialumo sutartį (NDA).