MOBILIŲ ĮRENGINIŲ VALDYMO (MDM) PASLAUGOS TEIKIMO TAISYKLĖS

1. Paslaugos apibrėžimas

1.1. Mobilių įrenginių valdymo (MDM) paslauga skirta užtikrinti Kliento organizacijos mobilių įrenginių (telefonų, planšečių ir kompiuterių) valdymą, saugumą ir kontrolę naudojant „Microsoft Intune“ platformą. Paslauga apima pirminį sprendimo diegimą, įrenginių registravimą, politikų taikymą, aplikacijų valdymą, nuotolinį administravimą bei bazinį saugumo užtikrinimą, siekiant apsaugoti organizacijos duomenis ir užtikrinti centralizuotą įrenginių valdymą.

1.2. Ši paslauga apima tik šiame dokumente aiškiai apibrėžtas MDM funkcijas ir negali būti interpretuojama kaip pilnas IT saugumo sprendimas, SOC paslauga, infrastruktūros administravimas ar naudotojų IT palaikymas, jei tai nėra numatyta atskirame susitarime.

2. Paslaugos apimtis

2.1. Pagrindinės MDM paslaugos

2.1.1. MDM sprendimo diegimas ir konfigūravimas

2.1.1.1. Kliento poreikių analizė.
2.1.1.2. Įrenginių analizė ir tinkamumo vertinimas.
2.1.1.3. „Microsoft Intune“ aplinkos konfigūravimas.
2.1.1.4. Įrenginių registracijos taisyklių ir politikų kūrimas (Apple, Android, Windows, macOS).
2.1.1.5. Autopilot konfigūracija - naujų įrenginių automatizuotam paruošimui (jei taikoma)
2.1.1.6. Politikų ir saugumo valdymas
2.1.1.7. Saugumo funkcijų ir politikų kūrimas (PIN/biometrija, diskų šifravimas).
2.1.1.8. Įrenginių atitikties (compliance) politikos.
2.1.1.9. Conditional Access taikymas (jei susieta su Entra ID)
2.1.1.10. OS atnaujinimų politikų kūrimas
2.1.1.11. Duomenų apsaugos (App Protection Policies) nustatymų konfigūravimas aplikacijų lygmeniu.

2.1.2. Aplikacijų ir konfigūracijų valdymas

2.1.2.1. Standartinių aplikacijų katalogo kūrimas.
2.1.2.2. Aplikacijų diegimas ir šalinimas.
2.1.2.3. Automatinio aplikacijų atnaujinimo politikų kūrimas.
2.1.2.4. Wi-Fi, VPN profilių konfigūravimas.

2.1.3. Įrenginių administravimas

2.1.3.1. Įrenginių registravimas į „Microsoft Intune“
2.1.3.2. Naujų įrenginių įtraukimas / senų pašalinimas.
2.1.3.3. Nuotolinis įrenginių valdymas.
2.1.3.4. Prarastų ar pavogtų įrenginių blokavimas, pilnas ar dalinis duomenų ištrynimas (wipe).

2.1.4. Ataskaitos ir naudotojų informavimas

2.1.4.1. Informacijos apie įrenginius ir aplikacijas teikimas
2.1.4.2. Periodinės ar „ad-hoc“ ataskaitos
2.1.4.3. MDM aplikos priežiūra
2.1.4.4. Naudotojų mokymas / instrukcijų rengimas (įrenginio registravimas, naudojimas).
2.1.4.5. Bazinės konsultacijos dėl MDM funkcionalumo.

2.2. Licencijavimas

2.2.1. Paslauga teikiama naudojant „Microsoft Intune“
2.2.2. Licencijos nėra įtrauktos į šią paslaugą – jos turi būti užsakomos atskirai.
2.2.3. Klientas atsakingas už licencijų įsigijimą ir galiojimą.
2.2.4. Reikalingos tinkamos Microsoft licencijos (pvz., „Microsoft 365 Business Premium“, E3/E5, EMS E3/E5).

2.3. Palaikomos operacinės sistemos

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

3. Paslaugos ribos

3.1. Paslauga teikiama naudojant standartinę „Microsoft Intune“ funkcionalumą.
3.2. Galimybės priklauso nuo OS ir gamintojo ribojimų.
3.3. Nepalaikomi nestandartiniai ar root/jailbreak įrenginiai.
3.4. Paslauga neapima:
3.4.1. Pilno IT saugumo stebėsenos (SOC, SIEM,MDR).
3.4.2. Tinklo, serverių ar infrastruktūros administravimo.
3.4.3. Verslo aplikacijų palaikymo.
3.4.4. Individualių sistemų integracijų.
3.4.5. Mobile App kūrimo ir palaikymo.
3.4.6. Incidentų tyrimų.
3.4.7. 24/7 stebėsenos.
3.5. MDM funkcionalumas priklauso nuo įrenginio gamintojo, modelio ir operacinės sistemos ribojimų,
3.6. „Heximus“ neatsako, jei įrenginių nepavyksta įregistruoti ar pritaikyti politikų dėl netinkamos OS versijos ar kitų techninių kliūčių,
3.7. Jei naudojama programinė įranga neturi palaikymo iš gamintojo arba jis pasibaigęs, „Heximus“ neprisiima atsakomybės už incidentų sprendimą,
3.8. Paslauga neužtikrina automatinės integracijos su kitomis trečiųjų šalių sistemomis, nebent tai iš anksto suderinta atskiru susitarimu. Trečiųjų šalių aplikacijų veikimas nėra garantuojamas.
3.9. Visi darbai, nepatenkantys į šios paslaugos apimtį vykdomi tik pagal atskirą užsakymą, apmokestinami papildomai ir derinami individualiai.

4. Atsakomybės ir sąlygos

4.1. Kliento atsakomybės
4.1.1. Užtikrinti licencijų įsigijimą ir galiojimą.
4.1.2. Užtikrinti įrenginių suderinamumą.
4.1.3. Informuoti apie prarastus įrenginius nedelsiant.
4.1.4. Užtikrinti darbuotojų laikymąsi saugumo politikų.
4.1.5. Naudoti legalią programinę įrangą.
4.2. „Heksimus“ atsakomybės
4.2.1. Vykdyti MDM konfigūraciją ir administravimą.
4.2.2. Taikyti politikas pagal susitarimą.
4.2.3. Teikti konsultacijas.
4.3. Atsakomybės ribojimas
4.3.1. „Heksimus“ neatsako už:
- „Microsoft Intune“, „Azure“ ar kitų platformų veikimą.
- OS ar įrenginių gamintorjų ribojimus.
- Nepavykusią registraciją dėl techninių apribojimų.
- Trečiųjų šalių aplikacijų veikimą.
- Jailbreak/root įrenginius.
4.4. Finansinė ir rizikos atsakomybė
4.4.1. „Heksimus“ neatsako už:
- Duomenų praradimą arba ištrynimą (pvz.: remote wipe)
- Saugumo incidentus už MDM ribų
- Netiesioginius nuostolius ar veiklos sustojimą.Konfigūracijų ir duomenų saugumas

4.5. Duomenų saugumas
4.5.1. Duomenų atsarginės kopijos nėra šios paslaugos dalis
4.5.2. Klientas atsako už informaciją įrenginiuose.
4.5.3. „Heximus“ vykdo veiksmus pagal Kliento instrukcijas
4.6. Priklausomybės nuo trečiųjų šalių
4.6.1. Paslauga priklauso nuo:
- Microsoft Intune.
- EntraID (Azure AD).
- OS gamintojų (Microsoft, Apple, Google).
4.6.2. Funkcionalumas gali keistis nepriklausomai nuo „Heksimus“.

5. Paslaugos teikimo režimas

5.1. Paslaugos teikimo režimas nurodytas „BENDROSIOS PASLAUGŲ TEIKIMO SĄLYGOS“ 1.3 ir 7.5 punktuose.
5.2. Žodiniai ar neformalūs prašymai nelaikomi galiojančiais.
5.3. „Heksimus“ turi teisę atmesti užklausą, jei ji:
- Viršija paslaugos apimtį.
- Prieštarauja „Microsoft“ gerosioms praktikoms.
- Kelia saugumo ar teisinę riziką.

6. Incidentų eskalacijos lygiai

6.1. 1 lygio pagalba (L1) – bazinė diagnostika.
6.2. 2 lygio pagalba (L2) – politikų ir konfigūracijų analizė.
6.3. 3 lygio pagalba (L3): eskalacija į „Microsoft“.
6.4. Eskalacija vykdoma pagal vidines procedūras: jei problema neišsprendžiama L1 lygyje per nustatytą laiką, ji perkeliama į L2, o prireikus – į L3.
6.5. Sprendimo laikas priklauso nuo gamintojo ir infrastruktūros.
6.6. Klientas informuojamas apie eskalacijos eigą, numatomą sprendimo laiką ir galimus veiklos apribojimus.

7. Paslaugos interpretavimo taisyklė

7.1. Paslauga interpretuojama tik pagal šiame dokumente nurodytą apimtį.
7.2. Bet koks platesnis interpretavimas laikomas negaliojančiu.
7.3. Visi papildomi lūkesčiai turi būti formalizuoti.