					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P27					Dokumendi pealkiri: **Pilveteenuste kasutamise poliitika**							
Versioon: 1.0		Jõustumiskuupäev: 01.01.2025			Dokumendi omanik:							
X	Poliitika		Standard		Protseduur		Vorm		Register		Muu	

Muudatuste ajalugu				
Muudatuse number	**Muudatuse kuupäev**	**Muudatused**	**Läbi vaadanud**	**Protsessi omanik**

Kinnitused			
Nimi	**Ametikoht**	**Kuupäev**	**Allkiri**

Õiguslik teatis (autoriõigus ja kasutuspiirangud)

(C) 2025 Clarysec LLC. All rights reserved.

Käesolev dokument on Clarysec LLC intellektuaalomand. Selle dokumendi ühtegi osa ei tohi ilma eelneva selgesõnalise kirjaliku loata kopeerida, taaskasutada, levitada ega muuta ärilistel või rakendamise eesmärkidel.

Loata kasutamine on rangelt keelatud ja võib kaasa tuua õiguslikke meetmeid.

Litsentsimise küsimustes võtke ühendust: info@clarysec.com

Kooskõla standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 8	Pilveteenuste operatiivse planeerimise ja ohje nõuded.
ISO/IEC 27002:2022	Kontrollimeetmed 5.23–5.25	Pilveteenuste kasutamise, poliitika ja turbega seotud nõuded.
NIST SP 800-53 Rev.5	AC-20, SA-9(5), SC-12–SC-28, SR-5	Väliste süsteemide kasutamine, lepingulised ja tehnilised nõuded, krüptograafilised kaitsemeetmed ning tarneahela kaitse.
ELi GDPR	Artiklid 28, 32, peatükk V	Pilveteenuse osutajana tegutseva volitatud töötleja nõuded, töötlemise turvalisus ja andmeedastus.
ELi NIS2	Artikkel 21(2)(f, i)	Kolmanda osapoole riskide ja tarneahela nõuded.
ELi DORA	Artiklid 5(2), 28	IKT ja kolmandate osapoolte teenuste (sh pilveteenuste) järelevalve finantssektori üksustes.
COBIT 2019	BAI04, DSS01, DSS05	Pilveteenuste käideldavus, operatsioonide juhtimine ja turbehaldus.

1. Eesmärk

1.1 Käesolev poliitika kehtestab organisatsioonis kohustuslikud nõuded pilveteenuste turvaliseks, nõuetele vastavaks ja vastutustundlikuks kasutamiseks teenusemudelites Infrastructure-as-a-Service (IaaS), Platform-as-a-Service (PaaS) ja Software-as-a-Service (SaaS).

1.2 Poliitika eesmärk on tagada, et pilveteenuseid võetakse kasutusele ja hallatakse viisil, mis kaitseb teabevarade konfidentsiaalsust, terviklust ja käideldavust ning täidab regulatiivseid, õiguslikke ja lepingulisi kohustusi.

1.3 Poliitika määratleb kontrollimeetmed pilveriskide ohjamiseks, andmete kaitsmiseks, teenuseosutajate vastavuse seireks ja lubamatu kasutuse kõrvaldamiseks. Samuti toetab see äriinnovatsiooni pilveplatvormide kaudu, viies kooskõlla turvalisuse, töökindluse ja kulutõhususe.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile töötajatele, töövõtjatele, kolmandatest osapooltest teenuseosutajatele ja väliskonsultantidele, kes organisatsiooni nimel võtavad pilveteenuseid kasutusele, konfigureerivad, haldavad, kasutavad või pääsevad neile juurde.

2.2 Poliitika kohaldub kõigile keskkondadele, kus töödeldakse organisatsiooni andmeid või töökoormusi, sealhulgas:

2.2.1 avaliku, privaatse, hübriid- ja kogukonnapilve juurutused;

2.2.2 kõik pilveteenuse mudelid (IaaS, PaaS, SaaS);

2.2.3 mitmepilvelahendused ja födereeritud arhitektuurid;

2.2.4 varjatud IT või isiklike pilvekontode kasutamine ärilistel eesmärkidel.

2.3 Poliitika hõlmab kõiki andmete klassifitseerimistasemeid ning kohaldub nii sisemistele süsteemidele kui ka tarnijate hallatavatele platvormidele, kus säilitatakse või töödeldakse organisatsioonile kuuluvaid või reguleeritud andmeid.

3. Eesmärgid

3.1 Tagada pilvetehnoloogiate turvaline ja järjepidev kasutamine selgelt määratletud kasutusjuhiste, turbe lähtekonfiguratsioonide ja juhtimisrollide kaudu.

3.2 Minimeerida pilveteenustega seotud tegevus- ja regulatiivseid riske, sealhulgas lubamatu juurdepääs, andmekaitserikkumised, väärkonfiguratsioonid, mittevastavus ja teenusekatkestused.

3.3 Kehtestada kõigile pilveteenuse osutajatele turbe- ja andmekaitsenõuded ning tõendada vastavust lepingutingimuste, hindamiste ja auditeerimisõiguste kaudu.

3.4 Võimaldada pilveteenuste skaleeritavat ja toimepidevat kasutuselevõttu, kahjustamata turvaseisundit, õiguslike nõuete täitmist ega talitluspidevust.

3.5 Viia pilveteenuste juhtimine ja kasutamine kooskõlla organisatsiooni ISMS-i raamistikuga, õiguslike kohustustega (nt GDPR, DORA), valdkondlike suuniste ja laialt tunnustatud heade tavadega (nt NIST, COBIT).

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 Kiidab heaks pilveteenuste kasutamise poliitika ja pilveteenuste strateegilise kasutuselevõtu tegevuskava.

4.1.2 Vaatab läbi ja kinnitab standardsetest pilveteenuste juhtimisnõuetest tehtavad kõrge riskiga erandid.

4.1.3 Tagab, et pilvealgatustel on piisav rahastus, järelevalve ja lõimitus ettevõtte riskijuhtimise raamistikku.

4.2 Infoturbejuht

4.2.1 Vastutab käesoleva poliitika ja organisatsiooni pilveteenuste registri eest.

4.2.2 Kinnitab uute pilveteenuse pakkujate kaasamise taustakontrolli ja riskihindamise alusel.

4.2.3 Vaatab läbi teenuseosutajate vastavusdokumentatsiooni ja valideerib vastavuse turbenõuetele.

[... Jaotised 4.3–8 ei ole selles eelvaates. Täieliku sisu saamiseks ostke täisdokument. ...]

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesolev poliitika tuleb läbi vaadata vähemalt üks kord aastas ja ajakohastada vastavalt vajadusele, et tagada jätkuv kooskõla järgmisega:

9.1.1 arenevad õiguslikud ja regulatiivsed nõuded (nt GDPR, NIS2, DORA);

9.1.2 muudatused standardites ISO/IEC 27001 või ISO/IEC 27002;

9.1.3 organisatsiooni pilvearhitektuuri, ohumaastiku või teenuseportfelli muudatused;

9.1.4 intsidendiuurimised, auditi tulemused või tegevuskogemusest saadud õppetunnid.

9.2 Läbivaatamise algatamise ja asjakohaste sidusrühmade kaasamise eest vastutab infoturbejuht, sealhulgas:

9.2.1 pilveturbe arhitekt;

9.2.2 õigus- ja vastavusmeeskond;

9.2.3 hanke- ja tarnijahalduse juhid;

9.2.4 teenuseomanikud ja IT-operatsioonid.

9.3 Kõik ajakohastused peavad olema:

9.3.1 versioonihaldusega ja kuupäevastatud;

9.3.2 tippjuhtkonna poolt heaks kiidetud;

9.3.3 teatavaks tehtud mõjutatud osapooltele, sealhulgas töötajatele, töövõtjatele ja kolmandatele osapooltele;

9.3.4 arhiveeritud kooskõlas sisemiste dokumentatsioonipoliitikatega.

9.4 Vahepealsed läbivaatused võivad olla algatatud järgmistel juhtudel:

9.4.1 uus koostöö pilveteenuse pakkujaga või suuremahulised migratsioonid;

9.4.2 uued ohud pilvetaristule;

9.4.3 olulised muudatused lepingulistes, õiguslikes või valdkondlikes kohustustes.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on tihedalt seotud järgmiste sisepoliitikatega ja sõltub neist:

10.1.1 P1 – infoturbepoliitika: kehtestab süsteemide ja teenuste turvalise toimimise üldpõhimõtted, mida käesolev poliitika pilvekontekstis rakendab.

10.1.2 P5 – muudatuste haldamise poliitika: kõik pilvekonfiguratsiooni muudatused peavad järgima P5-s sätestatud muudatuste ohje protseduure.

10.1.3 P13 – andmete klassifitseerimise ja märgistamise poliitika: määrab, kuidas andmeid enne pilve üleviimist hinnatakse ja kuidas rakendatakse kontrollimeetmeid, nagu krüptimine ja andmete asukoha piirangud.

10.1.4 P18 – krüptograafiliste kontrollimeetmete poliitika: sätestab krüptimise, võtmehalduse ja krüptograafiliste algoritmide kasutamise standardid, mida kohaldatakse vahetult pilveteenuste konfiguratsioonidele.

10.1.5 P22 – logimis- ja seirepoliitika: määratleb logide kogumise, säilitamise ja analüüsi nõuded, mida tuleb rakendada pilvekeskkondades.

10.1.6 P30 – intsidentidele reageerimise poliitika: määratleb pilveteenustega seotud turbesündmuste eskaleerimise, ohjeldamise ja parandusmeetmete protseduurid.

10.1.7 P33 – auditi ja nõuetele vastavuse seire poliitika: toetab auditivalmidust ja pidevat kindlust, et pilvekontrollimeetmed on rakendatud ja seiratavad.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001: punkt 8.1 – operatiivne planeerimine ja ohje: nõuab, et organisatsioon rakendaks ja juhiks protsesse, mis on vajalikud infoturbe nõuete täitmiseks, sealhulgas pilvekeskkondi hõlmavad protsessid.

11.2 ISO/IEC 27002:2022 – kontrollimeetmed 5.23 kuni 5.25:

11.2.1 Lisa A kontroll 5.23 – pilveteenuste kasutamine: nõuab riskipõhist hindamist, ametlikku autoriseerimist ja pilveteenuste kasutuse dokumenteerimist.

11.2.2 Lisa A kontroll 5.24 – pilveteenuste kasutamise poliitika: nõuab organisatsiooni vajaduste ja riskidega kooskõlas oleva ametliku pilveteenuste kasutamise poliitika kehtestamist ja rakendamist.

11.2.3 Lisa A kontroll 5.25 – turvalisus pilveteenustes: nõuab turbekontrollide lõimimist, lepingulisi kaitsemeetmeid ning pilvekeskkonnas majutatud töökoormuste ja andmete seiret.

11.3 NIST SP 800-53 Rev.5:

11.3.1 AC-20 – väliste süsteemide kasutamine: nõuab määratletud reegleid ja tingimusi organisatsiooni ressurssidele juurdepääsuks välistest või pilvekeskkonnas asuvatest süsteemidest.

11.3.2 SA-9(5) – välised infosüsteemide teenused: nõuab kolmanda osapoole pilvesüsteemidele lepingulisi turbenõudeid, järelevalvet ja pidevat seiret.

11.3.3 SC-12 kuni SC-28 – krüptograafilised kaitsemeetmed, piirikaitse ja edastuse terviklus: on kooskõlas pilvekeskkonnas majutatud teenuste ja edastatavate andmete krüptimise, identiteedi ja juurdepääsu nõuetega.

11.3.4 SR-5 – tarneahela kaitse: toetab teenuse osutamises osalevate pilveteenuse pakkujate hindamist ja lepingulist ohjet.

11.4 ELi GDPR (2016/679):

11.4.1 Artikkel 28 – volitatud töötleja kohustused: nõuab ametlikke lepinguid pilveteenuse pakkujatega, et tagada isikuandmete töötlemise turvalisus, konfidentsiaalsus ja auditivalmidus.

11.4.2 Artikkel 32 – töötlemise turvalisus: toetab pilvekeskkondades krüptimise, juurdepääsukontrolli, logimise ja muude kaitsemeetmete rakendamist.

11.4.3 Peatükk V – rahvusvahelised andmeedastused: nõuab andmete õiguspärast edastamist väljapoole ELi/EMPd, kasutades kaitsemeetmeid nagu standardsed lepingutingimused (SCC) või piisavuse otsused.

11.5 ELi NIS2 direktiiv (2022/2555):

11.5.1 Artikkel 21(2)(f, i): nõuab, et üksused juhiksid kolmandatest osapooltest pilveteenuse osutajatega seotud riske ning tagaksid digitaalse tarneahela tervikluse tehniliste ja korralduslike meetmete ning lepingutingimuste kaudu.

11.6 ELi DORA (2022/2554):

11.6.1 Artikkel 5(2) – IKT-riskide juhtimine: nõuab IKT kolmanda osapoole riskide, sealhulgas pilveteenustega seotud riskide, lõimimist üldisesse riskijuhtimisse.

11.6.2 Artikkel 28 – kriitiliste IKT kolmandast osapoolest teenuseosutajate järelevalve: nõuab, et finantssektori üksused seiraksid, kontrolliksid ja raporteeriksid pilveteenuse pakkujatega seotud sõltuvusi, turvaseisundit ja toimepidevust.

11.7 COBIT 2019:

11.7.1 BAI04 – käideldavuse ja mahu juhtimine: tagab, et pilveteenused on toimepidevad, seiratavad ja vastavad määratletud toimivuskriteeriumidele.

11.7.2 DSS01 – operatsioonide juhtimine: toetab operatiivset lõimimist, intsidentide käsitlemist ja konfiguratsiooni lähtealuste rakendamist pilvekeskkonnas majutatud platvormidel.

11.7.3 DSS05 – turbeteenuste juhtimine: suunab pilvespetsiifiliste turbekontrollide, seire ja intsidentide ennetamise rakendamist digitaalsete teenuste lõikes.