					Sisestage siia registreeritud juriidilise isiku nimi						
Dokumendi number: P04					Dokumendi pealkiri: **Juurdepääsukontrolli 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**

Kohaldatavad standardid ja regulatsioonid

Standard/regulatsioon	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 5.15, 5.17, 5.18	Loogilise ja füüsilise juurdepääsu haldus
ISO/IEC 27002:2022	Kontrollimeetmed 8.2, 8.3	Rollipõhine juurdepääs ja identiteedihaldus
NIST SP 800-53 Rev.5	AC-1 kuni AC-20, IA-1 kuni IA-8	Kontode ja juurdepääsu kontroll, identiteedi autentimine
ELi GDPR	Artiklid 5(1)(f), 32(1)(b); põhjendus 39	Isikuandmete kaitse ja minimeerimine
ELi NIS2	Artikkel 21(2)(c–e)	Juurdepääsukontroll, kasutajate autentimine ja varade kaitse
ELi DORA	Artiklid 6, 9(2)	IKT- ja kasutajate juurdepääs ning tugevad kontrollimeetmed / kolmandad osapooled
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Tööle asumine, käitlus, seire, vastavus

1. Eesmärk

1.1 Käesolev poliitika kehtestab kohustuslikud põhimõtted, vastutused ja kontrollinõuded infosüsteemidele, rakendustele, füüsilistele ruumidele ja andmevaradele juurdepääsu haldamiseks kogu organisatsioonis.

1.2 Poliitika tagab, et juurdepääs antakse ärivajaduse, tööülesannete ja riskitaseme alusel, rakendades vähimate õiguste, teadmisvajaduse ja tööülesannete lahususe põhimõtteid.

1.3 Käesolev poliitika toetab standardi ISO/IEC 27001:2022 punkti 5.15 ja seotud kontrollimeetmete rakendamist, mis reguleerivad loogilist ja füüsilist juurdepääsu, kasutajate autentimist ning juurdepääsu elutsükli haldust.

1.4 Käesolev poliitika toetab digitaalsete ja füüsiliste ressursside kaitset loata kasutamise, väärkasutuse või kompromiteerimise eest.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib kõigile kasutajatele, süsteemidele ja ruumidele ISMSi kohaldamisalas, sealhulgas:

2.1.1 töötajad, töövõtjad, tarnijad ja ajutine personal

2.1.2 kohapealne taristu, pilvekeskkonnas majutatud süsteemid ja hübriidkeskkonnad

2.1.3 kõik ettevõtte varad — riistvara, tarkvara, andmed ja turvatud füüsilised alad

2.1.4 loogiline juurdepääs (nt süsteemid, võrgud, rakendused, API-d) ja füüsiline juurdepääs (nt hooned, andmekeskused)

2.2 Käesolev poliitika reguleerib juurdepääsu kogu identiteedi ja ressursikasutuse elutsükli jooksul alates tööle asumisest ja õiguste andmisest kuni rollimuudatuste ja juurdepääsu lõpetamiseni.

2.3 Poliitika hõlmab ka isiklike seadmete kasutamise (BYOD) ja kaugjuurdepääsu juhtumeid, tagades kontrollimeetmete ühtsuse eri asukohtades ja seadmete omandimudelites.

3. Eesmärgid

3.1 Rakendada turvalised rollipõhised juurdepääsukontrollid, mis toetavad tegevuse terviklikkust ja vastavust regulatiivsetele nõuetele.

3.2 Tagada, et juurdepääsuõigused kinnitatakse, jälgitakse ja tühistatakse õigeaegselt.

3.3 Vältida loata juurdepääsu, õiguste eskaleerimist või aegunud juurdepääsuõiguste püsimist.

3.4 Rakendada vaikimisi nullusaldusel põhinevaid põhimõtteid, keelates juurdepääsu, kui see ei ole sõnaselgelt heaks kiidetud ja põhjendatud.

3.5 Anda audiitoritele ja sidusrühmadele kindlus tõenduspõhiste, automatiseeritud juurdepääsu ülevaatuste ja poliitika rakendamise kaudu.

3.6 Siduda juurdepääsukontroll äriprotsesside, personali elutsükli sündmuste ja tehniliste arhitektuuridega.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 Kinnitab juurdepääsukontrolli poliitika ning tagab selle rakendamiseks vajaliku eelarve ja ressursid.

4.1.2 Vaatab juhtkonna ülevaatuste käigus läbi juurdepääsukontrolli riskid ja määrab strateegilise taseme vastutuse.

4.2 CISO / ISMSi juht

4.2.1 Vastutab juurdepääsukontrolli raamistiku eest ning tagab selle kooskõla standardi ISO/IEC 27001 ja seotud standarditega.

4.2.2 Koordineerib poliitika rakendamist, kontrollimeetmete testimist ja juurdepääsukontrolli mõõdikute aruandlust.

4.2.3 Teostab järelevalvet riskipõhise juurdepääsumudeli üle ja jälgib süsteemseid kontrollilünki.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Läbivaatamise alused ja sagedus

9.1.1 Käesolev poliitika tuleb läbi vaadata:

9.1.1.1 kord aastas või

9.1.1.2 pärast olulist muudatust IT-taristus, regulatiivsetes nõuetes või riskitasemes

9.1.1.3 pärast intsidente, mis toovad esile nõrkused juurdepääsukontrollides

9.1.1.4 kui autentimistehnoloogiates või identiteediplatvormides toimuvad olulised muutused

9.2 Läbivaatamise vastutus ja protsess

9.2.1 CISO või määratud ISMSi eestvedaja haldab läbivaatamistsüklit, kaasates järgmise:

9.2.1.1 siseauditi tähelepanekud

9.2.1.2 juurdepääsu läbivaatamise tulemused ja mõõdikud

9.2.1.3 õiguslikud ja regulatiivsed uuendused

9.2.1.4 tehnoloogiaplatvormide muudatused

9.2.2 Kõik muudatused peab heaks kiitma tippjuhtkond ning need tuleb edastada kõigile sidusrühmadele.

9.2.3 Oluliste muudatuste korral võib mõjutatud kasutajatelt nõuda poliitika uuesti kinnitamist.

9.3 Versioonihaldus ja dokumenteerimine

9.3.1 Põhiversiooni tuleb säilitada ISMSi dokumendihoidlas koos järgmiste metaandmetega:

9.3.1.1 versiooninumber ja muudatuste logi

9.3.1.2 jõustumiskuupäev ja järgmise läbivaatamise kuupäev

9.3.1.3 omanik ja kinnitaja

9.3.1.4 levitamise ja kinnitamise kirjed

9.3.2 Asendatud versioonid tuleb arhiveerida ja hoida kättesaadavana vähemalt 3 aastat.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika sõltub funktsionaalselt järgmistest poliitikatest ning seda tuleb tõlgendada koos nendega:

10.1.1 P01 – Infoturbe poliitika: määratleb organisatsiooni turbepõhimõtted ja kõrgtaseme ootused juurdepääsukontrollile.

10.1.2 P03 – Aktsepteeritava kasutuse poliitika: sätestab käitumuslikud tingimused juurdepääsule ja kasutaja vastutuse süsteemide nõuetekohase kasutamise eest.

10.1.3 P05 – Muudatuste halduse poliitika: reguleerib, kuidas juurdepääsuseadete, rollide või grupistruktuuride muudatused tuleb turvaliselt rakendada ja testida.

10.1.4 P07 – Tööle asumise ja töösuhte lõpetamise poliitika: käivitab juurdepääsuõiguste andmise ja tühistamise vastavalt kasutaja elutsükli sündmustele.

10.1.5 P11 – Kasutajakontode ja õiguste halduse poliitika: rakendab kontotaseme kontrollimeetmeid ja täiendab käesolevat poliitikat tehnilise juurdepääsu rakendamise juhistega.

10.2 Koos moodustavad need poliitikad sidusa ja rakendatava juurdepääsu juhtimise raamistiku eri äriüksuste ja tehnoloogiate lõikes.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001:2022:

11.1.1 Punkt 5.15 – Juurdepääsukontroll: käesolev poliitika täidab nõude kontrollida juurdepääsu teabele ja muudele seotud varadele äriliste ning infoturbenõuete alusel.

11.1.2 Punkt 5.17 – Identiteedihaldus ja punkt 5.18 – Autentimisteave: neid rakendatakse identiteediõiguste määramise, autentimismehhanismide ja õiguste omistamise kaudu.

11.1.3 Lisa A kontrollimeetmed 8.2 (Juurdepääsukontrolli poliitika) ja 8.3 (Identiteedihaldus): annavad aluse käesoleva poliitika kontrollieesmärkidele, sealhulgas rollipõhine juurdepääs, kasutaja elutsükli integreerimine ja privilegeeritud juurdepääsu kaitse.

11.2 NIST SP 800-53 Rev.5:

11.2.1 AC perekond (AC-1 kuni AC-20): käesolev poliitika toetab NISTi juurdepääsukontrolli nõudeid nii füüsilistele kui ka loogilistele süsteemidele, sealhulgas poliitika määratlemine (AC-1), kontohaldus (AC-2) ja tööülesannete lahusus (AC-5).

11.2.2 IA perekond (IA-1 kuni IA-8): annab juhised identiteedi autentimiseks, autentimisandmete kaitseks ja MFA kasutamiseks.

11.2.3 AU-2, AU-12: käesoleva poliitika alusel rakendatavad logimise ja auditeerimise nõuded toetavad kasutaja vastutust ja intsidentide uurimist.

11.2.4 PE-2 kuni PE-6: käsitlevad füüsilise juurdepääsu piiranguid, mida käesolev poliitika rakendab osaliselt läbipääsukaartide kontrolli ja hoonetele juurdepääsuõiguste kaudu.

11.3 ELi GDPR (2016/679):

11.3.1 Artikkel 5(1)(f): isikuandmeid tuleb kaitsta loata juurdepääsu eest. Käesolev poliitika tagab selle põhimõtte tehnilise ja protseduurilise rakendamise.

11.3.2 Artikkel 32(1)(b): nõuab juurdepääsukontrollide, pseudonüümimise ja krüpteerimise rakendamist, et vältida isikuandmete loata töötlemist.

11.3.3 Põhjendus 39: nõuab isikuandmetele juurdepääsu minimeerimist, mida siin rakendatakse vähimate õiguste põhimõtte ja juurdepääsu põhjendamise nõuete kaudu.

11.4 ELi NIS2 direktiiv (2022/2555):

11.4.1 Artikkel 21(2)(c–e): käesolev poliitika võimaldab tehniliste ja korralduslike meetmete rakendamist juurdepääsukontrolli, kasutajate autentimise ja varade kaitse jaoks olulistes ja tähtsates üksustes.

11.5 ELi DORA (2022/2554):

11.5.1 Artikkel 6: nõuab IKT-riskijuhtimise poliitikaid, mis hõlmavad sõnaselgelt kasutajate juurdepääsu haldust ja identiteedi elutsükli kontrollimeetmeid. Käesolev poliitika täidab selle nõude finants- ja IKT-teenuste sektoris.

11.5.2 Artikkel 9(2): käesolev poliitika toetab tugevate juurdepääsukontrollide rakendamist kolmandate osapoolte ja kontsernisisese IKT-teenuste halduse osana.

11.6 COBIT 2019:

11.6.1 APO07 – Personalijuhtimise haldamine: rakendab tööle asumise ja lahkumise kontrollimeetmeid juurdepääsu juhtimise toetamiseks.

11.6.2 BAI03 – Lahenduste tuvastamise ja arenduse haldamine: seob juurdepääsukontrolli nõuded süsteemikavandi ja muudatuste protsessidega.

11.6.3 DSS01 – Käitluse haldamine ja DSS05 – Turvateenuste haldamine: reguleerivad loogilise juurdepääsu piirangute rakendamist ja rikkumiste seiret.

11.6.4 MEA03 – Vastavuse seire, hindamine ja kontroll: toetab auditit ja kindlustandvaid mehhanisme juurdepääsukontrolli tulemuslikkuse tõendamiseks.