					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P04S					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**

Kooskõla kohaldatavate standardite ja regulatsioonidega

Standard/regulatsioon	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 5	
ISO/IEC 27002:2022	Kontrollimeetmed 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 kuni AC-5	
ELi isikuandmete kaitse üldmäärus (GDPR)	Artikkel 32	
ELi NIS2 direktiiv	Artikkel 21 lõige 2 punkt b	
ELi DORA määrus	Artikkel 9	
COBIT 2019	APO07, DSS01	

1. Eesmärk

1.1. Käesolev poliitika määratleb, kuidas organisatsioon haldab juurdepääsu süsteemidele, andmetele ja ruumidele, et tagada teabele juurdepääs üksnes volitatud isikutele vastavalt tööalasele vajadusele.

1.2. Poliitika kehtestab selged nõuded kasutajakontode loomiseks, muutmiseks, seireks ja eemaldamiseks, et vähendada volitamata juurdepääsu riski ning toetada kohaldatavate õigusaktide ja standardite järgimist.

1.3. Poliitika lähtub vähimate õiguste põhimõttest, mille kohaselt peab juurdepääs piirduma tööülesannete täitmiseks vajaliku miinimumiga.

2. Kohaldamisala

2.1. Käesolev poliitika kehtib kõigile isikutele, kes kasutavad või haldavad juurdepääsu organisatsiooni IT-süsteemidele, võrkudele, andmetele või ruumidele, sealhulgas:

2.1.1. töötajad

2.1.2. töövõtjad

2.1.3. ajutised töötajad

2.1.4. välised IT-teenuse osutajad

2.2. Poliitika hõlmab juurdepääsu järgmisele:

2.2.1. ettevõtte rakendused, failijagamised ja andmebaasid

2.2.2. e-post, VPN ja kaugjuurdepääsusüsteemid

2.2.3. äritegevuses kasutatavad pilveteenused

2.2.4. füüsiline juurdepääs turvatud ruumidele, näiteks kontoritele või serveriruumidele

2.3. Käesolev poliitika on siduv kõikide seadmete (ettevõtte väljastatud või heaks kiidetud BYOD-seadmed), platvormide ja asukohtade puhul.

3. Eesmärgid

3.1. Tagada, et juurdepääsuõigused antakse üksnes pärast ametlikku kinnitamist rolli ja ärilise põhjenduse alusel.

3.2. Vältida volitamata või ülemäärast juurdepääsu tundlikele andmetele, süsteemidele või taristule.

3.3. Määratleda selged protseduurid kasutajate juurdepääsu andmiseks, muutmiseks ja lõpetamiseks.

3.4. Nõuda regulaarset juurdepääsuõiguste läbivaatamist ning automatiseeritud või käsitsi peetavat logimist auditi toetamiseks.

3.5. Toetada juurdepääsupiirangute tehnilist rakendamist seadistuste ja seire abil.

4. Rollid ja vastutusalad

4.1. Tegevjuht

4.1.1. Kinnitab käesoleva poliitika ja tagab, et tõhusate juurdepääsukontrollimeetmete rakendamiseks on olemas vajalikud ressursid.

4.1.2. Kinnitab erandid ja vaatab läbi iga-aastaste juurdepääsuauditite tulemused.

4.2. IT-juht / väline IT-teenuse osutaja

4.2.1. Korraldab kasutajakontode loomise, muutmise ja sulgemise.

4.2.2. Haldab juurdepääsukontrolli registrit, kuhu kantakse kõik toimingud (loomine, muutmine, eemaldamine).

4.2.3. Rakendab rollipõhist juurdepääsukontrolli (RBAC) ja nõuab tugevat autentimist (nt MFA).

4.2.4. Vaatab läbi juurdepääsuloge kahtlase tegevuse tuvastamiseks ja teavitab probleemidest tegevjuhti.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1. Poliitika iga-aastane läbivaatamine

9.1.1. IT-juht peab käesoleva poliitika läbi vaatama vähemalt kord aastas. Kõik muudatused õiguslikus, tehnilises või organisatsioonilises kontekstis peavad käivitama viivitamatu ajakohastamise.

9.2. Läbivaatamise ajendid

9.2.1. Poliitika tuleb läbi vaadata ka siis, kui esineb mõni järgmistest asjaoludest:

9.2.2. olulised süsteemimuudatused või pilveteenustele üleminek

9.2.3. muudatused rollides või organisatsioonistruktuuris

9.2.4. turvaintsident, mis hõlmab volitamata juurdepääsu

9.2.5. regulatiivsed muudatused (nt GDPR-i, NIS2 või DORA uuendused)

9.3. Muudatuste dokumenteerimine ja teavitamine

9.3.1. Muudatused tuleb logida koos versiooniajalooga, tegevjuhi kinnitusega ning edastada kõigile asjaomastele töötajatele.

9.4. Kättesaadavus ja koolitus

9.4.1. Käesolev poliitika peab olema kättesaadav kõigile töötajatele ning asjakohane koolitus tuleb korraldada sisseelamise käigus ja seejärel kord aastas.

10. Seotud poliitikad ja seosed

10.1. Käesolevat poliitikat tuleb turvaliste juurdepääsutavade täielikuks rakendamiseks kohaldada koos järgmiste VKE poliitikatega:

10.1.1. P3S – Aktsepteeritava kasutuse poliitika: tagab, et kasutajad mõistavad neile antud juurdepääsuga seotud lubatud käitumist.

10.1.2. P5S – Muudatuste juhtimise poliitika: tagab, et juurdepääsuõigused on kooskõlas heakskiidetud süsteemimuudatustega.

10.1.3. P7S – Tööle asumise ja töösuhte lõpetamise poliitika: määratleb kasutajatele juurdepääsu andmise ja eemaldamise käivitavad sündmused.

10.1.4. P17S – Andmekaitse ja privaatsuse poliitika: tagab, et juurdepääsukontrollimeetmed on kooskõlas isikuandmete kaitse meetmetega.

10.1.5. P30S – Intsidendihalduse poliitika: määratleb, kuidas juurdepääsuga seotud intsidente (nt väärkasutus või rikkumised) hallatakse ja uuritakse.

11. Viitestandardid ja raamistikud

11.1. ISO/IEC 27001

11.1.1. Punkt 5.15 – nõuab formaliseeritud juurdepääsukontrolli poliitikaid ja protsesse.

11.2. ISO/IEC 27002

11.2.1. Kontrollimeetmed 5.15–5.17 – määratlevad üksikasjalikud juhised rollipõhise juurdepääsu, kasutajakonto elutsükli halduse ja privilegeeritud juurdepääsu käsitlemise kohta.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 kuni AC-5 – nõuavad struktureeritud poliitikaid juurdepääsu haldamiseks, sealhulgas kontode volitamiseks, läbivaatamiseks ja seireks.

11.4. ELi isikuandmete kaitse üldmäärus (GDPR)

11.4.1. Artikkel 32 – nõuab tehniliste ja korralduslike meetmete rakendamist (näiteks juurdepääsu haldamine), et tagada andmete turvalisus ja konfidentsiaalsus.

11.5. ELi NIS2 direktiiv

11.5.1. Artikkel 21 lõige 2 punkt b – nõuab operatiivseid juurdepääsukontrolle ja identiteedihalduse süsteeme, et vältida volitamata juurdepääsu süsteemidele.

11.6. ELi DORA määrus

11.6.1. Artikkel 9 – rõhutab IKT-riskide turvalist juhtimist, sealhulgas tugevat juurdepääsukontrolli finantssektori üksustes.

11.7. COBIT 2019

11.7.1. APO07 – hallatud personal: nõuab juurdepääsuga seotud vastutuste määratlemist ja rakendamist.

11.7.2. DSS01 – toimingute haldamine: hõlmab loogilise juurdepääsu haldamise protseduure ja turvalise töökeskkonna säilitamist.