					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P11					Dokumendi pealkiri: **kasutajakontode ja õiguste haldamise 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 standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 6.1.3, punkt 8	-
ISO/IEC 27002:2022	Kontrollimeetmed 5.15-5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2 - IA-5, AU-2, AU-12	-
ELi GDPR	Artikkel 5(1)(f), 32; põhjendus 39	-
ELi NIS2	Artikkel 21(2)(a, d), 21(3)	-
ELi DORA	Artikkel 5, 9	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Eesmärk

1 Käesolev poliitika kehtestab kohustuslikud kontrollimeetmed kasutajakontode ja õiguste haldamiseks kõigis teabesüsteemides ja teenustes. Sellega tagatakse, et juurdepääs organisatsiooni ressurssidele antakse valideeritud identiteedi, rollipõhise vajaduse, vähimate õiguste põhimõtte ja tööülesannete lahususe alusel.

1.1 See toetab organisatsiooni pühendumust infoturbele, rakendades struktureeritud ja auditivalmis protsesse kasutajakontode loomiseks, õiguste määramiseks, kasutuse seireks ja kontode sulgemiseks.

1.2 Käesolev poliitika on kriitilise tähtsusega loata juurdepääsu, õiguste väärkasutuse, siseohtude ja kohaldatavate regulatiivsete raamistike nõuetele mittevastavuse riski vähendamiseks.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile töötajatele, töövõtjatele, kolmandatest osapooltest teenuseosutajatele, konsultantidele ja muudele isikutele, kellele on antud juurdepääs organisatsiooni IT-ressurssidele, rakendustele või andmetele.

2.2 See reguleerib kõiki süsteeme ja keskkondi, kus rakendatakse kasutajate autentimise ja juurdepääsukontrolli mehhanisme, sealhulgas, kuid mitte ainult:

2.2.1 ettevõtte rakendused ja andmebaasid

2.2.2 pilveplatvormid ja SaaS-keskkonnad

2.2.3 operatsioonisüsteemid ja halduskonsoolid

2.2.4 kaugjuurdepääsu tööriistad ja VPN-ühendused

2.2.5 identiteedi- ja juurdepääsuhalduse (IAM) süsteemid

2.3 Poliitika hõlmab nii tavakasutajakontosid kui ka privilegeeritud kasutajakontosid ning sisaldab kontrollimeetmeid järgmise üle:

2.3.1 kontode loomine, muutmine ja deaktiveerimine

2.3.2 õiguste eskaleerimine ja delegeerimine

2.3.3 seansside kontroll ja seire

2.3.4 autentimismeetodid ja autentimisandmete haldus

3. Eesmärgid

3.1 Tagada, et kõik kasutajakontod oleksid üheselt tuvastatavad, nõuetekohaselt volitatud ja määratud üksnes pärast vajaduse ametlikku valideerimist.

3.2 Rakendada vähimate õiguste põhimõtet ja vältida ebavajalikku või ülemäärast juurdepääsu, kehtestades ranged kontrollimeetmed privilegeeritud kontode andmisele ja kasutamisele.

3.3 Nõuda kasutajakonto staatuse õigeaegset ajakohastamist töösuhte või rollimuudatuste alusel, sealhulgas viivitamatut deaktiveerimist töösuhte lõppemisel.

3.4 Võimaldada kasutuseta, väärkasutatud või loata kontode ennetavat tuvastamist ja kõrvaldamist logimise, ülevaatuste ja automatiseerimise abil.

3.5 Tagada kooskõla standardiga ISO/IEC 27001:2022 ja seotud standarditega ning täita asjakohastest õiguslikest ja regulatiivsetest raamistikest, nagu GDPR, NIS2, DORA ja COBIT 2019, tulenevaid kohustusi.

4. Rollid ja vastutused

4.1 infoturbe juht (CISO)

4.1.1 Vastutab käesoleva poliitika eest ja tagab selle rakendamise kogu organisatsioonis.

4.1.2 Vaatab läbi ja kiidab heaks kõik ametlikud erandid või erakorralise juurdepääsu juhtumid.

4.1.3 Esitab kontodega seotud auditileiud ja eskaleerib riskid tippjuhtkonnale.

4.2 juurdepääsuhalduse juht / IT-administraator

4.2.1 Haldab ja käitab kasutajakontode elutsükli haldamise tehnilisi kontrollimeetmeid.

4.2.2 Viib heakskiidetud taotluse alusel ellu juurdepääsuõiguste andmise, lõpetamise ja õiguste haldamise toimingud.

4.2.3 Hoiab ajakohasena kõigi kasutajakontode, nende staatuse ja õiguste taseme autoriteetset registrit.

4.2.4 Toetab auditeid ja vastavuse ülevaatusi logide ning tegevusaruannetega.

[... 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 kord aastas või oluliste muudatuste korral järgmises:

9.1.1 organisatsiooniline struktuur või äriprotsessid

9.1.2 IT-süsteemid, identiteediplatvormid või juurdepääsumeetodid

9.1.3 identiteedi- ja juurdepääsuhaldusega seotud regulatiivsed või lepingulised nõuded

9.2 Infoturbe juht (CISO) vastutab koos juurdepääsuhalduse juhiga läbivaatamisprotsessi algatamise ja sidusrühmade tagasiside koordineerimise eest.

9.3 Vahepealse läbivaatamise võivad käivitada:

9.3.1 kasutajakontode väärkasutusega seotud turvaintsidendid

9.3.2 auditileiud, mis toovad esile puudused kontode elutsükli haldamises

9.3.3 uute identiteedihalduse või privilegeeritud juurdepääsu halduse tööriistade juurutamine

9.4 Käesoleva poliitika ajakohastused peavad olema:

9.4.1 versioonihalduse all ja registreeritud ISMS-i dokumentatsioonihoidlas

9.4.2 edastatud kõigile asjakohastele sidusrühmadele, sealhulgas osakonnajuhtidele, IT-operatsioonidele ja personaliosakonnale

9.4.3 toetatud ajakohastatud koolitusmaterjalide ja protseduurijuhistega

9.5 Kõik muudatused peab heaks kiitma tippjuhtkond või infoturbe juhtkomitee (ISSC) ning need tuleb auditi eesmärgil logida.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika on operatiivselt seotud järgmiste ISMS-i poliitikakomplekti kuuluvate poliitikatega ning seda toetavad järgmised poliitikad:

10.1.1 P4 juurdepääsukontrolli poliitika: kehtestab juurdepääsukontrolli üldpõhimõtted ja mehhanismid, sealhulgas reeglipõhised ja rollipõhised kontrollimeetmed.

10.1.2 P7 töölevõtu ja töösuhte lõpetamise poliitika: kirjeldab protseduurilisi samme kasutaja juurdepääsu algatamiseks ja lõpetamiseks kooskõlas HR-tegevustega.

10.1.3 P8 infoturbeteadlikkuse ja koolituse poliitika: tugevdab kasutajate vastutust konto turvalisuse ja autentimisandmete kaitsmise eest.

10.1.4 P13 andmete klassifitseerimise ja märgistamise poliitika: suunab juurdepääsutasemeid andmete klassifitseerimise alusel, tagades, et õiguste piirid vastavad tundlikkuse tasemetele.

10.1.5 P22 logimise ja seire poliitika: tagab, et auditijäljed kogutakse kõigi kontodega seotud tegevuste kohta ning vaadatakse üle anomaaliate või loata kasutuse tuvastamiseks.

10.1.6 P30 intsidentidele reageerimise poliitika (P30): reguleerib eskaleerimist, ohjeldamist ja intsidendijärgseid tegevusi õiguste väärkasutuse või loata kontotegevuse korral.

10.2 Kõik need poliitikad toimivad koos, et rakendada organisatsioonis sidusat ja riskipõhist identiteedi- ning juurdepääsuhalduse raamistikku.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas ülemaailmselt tunnustatud küberturbe standardite ja regulatiivsete raamistikega, mis nõuavad identiteedi, juurdepääsu ja õiguste turvalist haldamist organisatsiooni infoturbe põhikomponendina.

11.2 ISO/IEC 27001:

11.2.1 Punkt 6.1.3 nõuab, et organisatsioonid määraksid kindlaks, hindaksid ja käsitleksid infoturberiske, muutes juurdepääsu ja õiguste haldamise ametlikuks riskipõhiseks kontrollimeetmeks, mis on lõimitud ISMS-i planeerimisprotsessi.

11.2.2 Punkt 8.1 – operatiivne planeerimine ja kontroll: rõhutab tehniliste ja protseduuriliste kaitsemeetmete rakendamist, mis reguleerivad kasutajate ja privilegeeritud juurdepääsu.

11.3 ISO/IEC 27002:2022 – kontrollimeetmed 5.15 kuni 5.18:

11.3.1 Kontroll 5.15 – kasutajate juurdepääsuhaldus: toetab ametlikke protsesse kasutajakontode loomiseks, juurdepääsu volitamiseks ja juurdepääsuõiguste perioodiliseks ülevaatamiseks.

11.3.2 Kontroll 5.16 – identiteedihaldus: kehtestab identiteedi unikaalsuse, elutsükli kontrollimeetmed ja turvalise autentimise rakendamise.

11.3.3 Kontroll 5.17 tagab, et privilegeeritud juurdepääsuõiguste andmine ja kasutamine on kogu kasutajakonto elutsükli vältel rangelt kontrollitud, jälgitav ja kooskõlas vähimate õiguste põhimõttega.

11.3.4 Kontroll 5.18 – privilegeeritud juurdepääsuõigused: täielikult kaetud rollipõhise õiguste määramise, auditite ja kõrgendatud juurdepääsu heakskiitmise nõuetega.

11.4 Need kontrollimeetmed suunavad kasutajakontode registreerimise, registrist eemaldamise, õiguste lahususe ja autentimisteabe kasutamise struktureeritud rakendamist. Poliitika jõustab identiteedi elutsükli juhtimist, õigeaegselt antavat juurdepääsu ja kõrgendatud seansside seiret, et vältida süsteemide loata kasutamist.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (juurdepääsukontrolli poliitika) ja AC-2 (kontode haldamine): kaetud poliitikanõuetega juurdepääsu heakskiitude, rollide vastendamise ja kasutajakontode auditite kohta.

11.5.2 AC-5 (tööülesannete lahusus) ja AC-6 (vähimad õigused): täidetud õiguste piiramise, töörollidega vastavusse viimise ja kõrge riskiga ülesannete kahekordse heakskiiduga.

11.5.3 IA-2 kuni IA-5 (tuvastamine ja autentimine): rakendatud tugeva autentimise mehhanismide, autentimisandmete elutsükli reeglite ja MFA nõuete kaudu.

11.5.4 AU-2, AU-12 (auditilogimine ja analüüs): kaetud seansside salvestamise ja privilegeeritud tegevuse seire kaudu tundlikes keskkondades.

11.6 ELi GDPR (2016/679):

11.6.1 Artikkel 32 – töötlemise turvalisus: nõuab juurdepääsukontrolle ja identiteedi kontrollimise mehhanisme isikuandmete kaitseks. See on täidetud konto heakskiitmise, õiguste ülevaatamise ja tugeva autentimise kaitsemeetmete nõudmise kaudu.

11.6.2 Artikkel 5(1)(f) – terviklus ja konfidentsiaalsus: tagab, et isikuandmetele pääsevad ligi ainult volitatud kasutajad õiguspäraste rollide alusel, mida tugevdab kontohalduse rakendamine.

11.6.3 Põhjendus 39: nõuab selget juurdepääsu piiramist ja vastutust; käesolev poliitika toetab kasutajaidentiteetide ja õiguste määrangute täielikku jälgitavust.

11.7 ELi NIS2 direktiiv (2022/2555):

11.7.1 Artikkel 21(2)(a, d): nõuab, et üksused rakendaksid juurdepääsuhalduse poliitikaid ning autentimisandmete ja privilegeeritud seansside turvalist käsitlemist, mida toetavad käesoleva poliitika juurdepääsuõiguste andmise, seire ja erandite kontrollimeetmed.

11.7.2 Artikkel 21(3): edendab juurdepääsudistsipliini ja tugevat identiteedikindlust kriitilistes sektorites; see on täidetud unikaalsete identifikaatorite, RBAC-i ja ajaliselt piiratud kõrgendatud juurdepääsu kasutamisega.

11.8 ELi DORA (2022/2554):

11.8.1 Artikkel 5 – IKT juhtimine ja kontroll: nõuab IKT kasutajahalduses formaliseeritud protsesse, mis on kaetud dokumenteeritud kasutajakontode loomise, deaktiveerimise ja erandite käsitlemisega.

11.8.2 Artikkel 9 – IKT-riskide juhtimine: suunab organisatsioone süsteeme kaitsma juurdepääsupiirangute ja seire abil; see on käsitletud MFA, privilegeeritud juurdepääsu logimise ja tsentraliseeritud ülevaatuste kaudu.

11.9 COBIT 2019:

11.9.1 DSS01 – hallatud operatsioonid: edendab standardiseeritud operatiivsete kontrollimeetmete rakendamist, sealhulgas kasutajakontode elutsükli haldust ja juurdepääsu dokumenteerimist.

11.9.2 DSS05 – hallatud turbeteenused: kajastab kasutajate ja süsteemide õiguste turvalist administreerimist, toetades riskide maandamist vähimate õiguste põhimõtte ja auditijälje valideerimise kaudu.

11.9.3 APO13 – hallatud turve: nõuab juurdepääsuhalduse rakendamist digivarade kogu ulatuses; see on täidetud kasutajakontode ja rollide volitamise ametlike tavade ning perioodiliste ülevaatamise nõuetega.