					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P11S					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 õigusaktidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 5.3, 8	Rollid, vastutused ning kasutajate juurdepääsuhalduse operatiivne kavandamine ja kontroll
ISO/IEC 27002:2022	Kontroll 8	Kontrollimeetmed kõrgendatud õiguste määramiseks, läbivaatamiseks ja eemaldamiseks
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Kontode loomine, seire, vähimate õiguste põhimõte ja tööülesannete lahusus
EL NIS2	Artikkel 21(2)(d)	Kasutajate juurdepääsuhaldus elutähtsate ja oluliste üksuste jaoks
EL DORA	Artikkel 9(2)(b)	Privilegeeritud juurdepääsu kontroll finantssektori üksustes
COBIT 2019	DSS05.03, DSS05.04	Juurdepääsuõiguste andmine, juurdepääsu lõpetamine ja kasutajate juurdepääsu perioodiline läbivaatamine
EL GDPR	Artikkel 32	Asjakohased juurdepääsukontrollid isikuandmete kaitseks

1. Eesmärk

1.1 Käesolev poliitika kehtestab reeglid kasutajakontode ja juurdepääsuõiguste haldamiseks turvalisel, ühtsel ja jälgitaval viisil. See tagab, et süsteemidele ja andmetele on juurdepääs ainult volitatud kasutajatel ning et juurdepääs vastab nende rollile ja vastutusele.

1.2 Tõhus kontode ja õiguste haldamine on oluline, et ennetada loata juurdepääsu, vähendada siseohtusid ning tagada vastavus ISO/IEC 27001-le, GDPR-ile ja muudele regulatiivsetele nõuetele.

1.3 Käesolev poliitika võimaldab organisatsioonil määratleda kontode kasutamise omandiõiguse ja vastutuse, seirata ning auditeerida õiguste eskaleerimist ning piirata või tühistada juurdepääsu turvaliselt, kui seda enam ei vajata.

1.4 Samuti kaitseb see äritegevust operatiivsete vigade või väärkasutuse eest, mis tulenevad ülemäärasest või seireta juurdepääsust, ning aitab vähendada juhuslike andmeleketega, õiguste väärkasutusega või regulatiivse mittevastavusega seotud riske.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmistele isikutele ja objektidele:

2.1.1 Kõik töötajad, praktikandid, töövõtjad ja kolmandate isikute kasutajad, kellel on juurdepääs organisatsiooni IT-süsteemidele

2.1.2 Kõik süsteemid, seadmed, teenused ja platvormid, mida organisatsioon haldab ise või enda nimel, sealhulgas pilveplatvormid, kohapealne taristu ja kolmanda osapoole tööriistad

2.2 See hõlmab kõiki kasutajakontode liike, sealhulgas:

2.2.1 Nimelised kasutajakontod (nt e-posti kontod, süsteemi sisselogimised)

2.2.2 Administraatori- ja süsteemitaseme kontod

2.2.3 Ajutised, külalis- või kolmandate isikute autentimistunnused

2.2.4 Teenusekontod, mida kasutavad rakendused või automatiseeritud süsteemid

2.3 Poliitika kehtib kogu konto elutsükli jooksul alates loomisest ja kinnitamisest kuni muutmise, seire ja deaktiveerimiseni. See hõlmab esmast juurdepääsuõiguste andmist tööle asumisel, juurdepääsuõiguste ülevaatamist rollimuudatuste korral ning juurdepääsuõiguste tühistamist lahkumisprotsessi käigus.

3. Eesmärgid

3.1 Määrata kõigile süsteemikasutajatele unikaalsed ja jälgitavad kasutajaidentiteedid, tagades vastutuse ja välistades sõltuvuse jagatud autentimisandmetest.

3.2 Rakendada vähimate õiguste põhimõtet, tagades, et kasutajatele antakse ainult nende tööülesannete täitmiseks vajalik minimaalne juurdepääsutase.

3.3 Ennetada loata juurdepääsu tundlikele süsteemidele või andmetele selgelt dokumenteeritud kinnitamis- ja läbivaatamisprotsesside kaudu.

3.4 Tagada kasutajakontode õigeaegne deaktiveerimine, kui neid enam ei vajata, näiteks töösuhte lõppemisel, lepingu lõppemisel või rollimuudatuse korral.

3.5 Säilitada turvaline ja auditivalmis keskkond, dokumenteerides kõik kontomuudatused, kinnitused ja perioodilised läbivaatamised.

3.6 Tagada, et õiguste eskaleerimine on rangelt kontrollitud, sõltumatult kinnitatud ja logitud ning et kõrgendatud juurdepääs tühistatakse viivitamata, kui seda enam ei vajata.

4. Rollid ja vastutused

4.1 Tegevjuht (GM)

4.1.1 Vastutab käesoleva poliitika rakendamise üldise korraldamise eest.

4.1.2 Tagab, et kontohalduse praktikad on kooskõlas ISO/IEC 27001 sertifitseerimisnõuete ja asjakohaste õiguslike kohustustega (nt GDPR).

4.1.3 Teda tuleb viivitamata teavitada igast loata juurdepääsust, turvaintsidendist või kasutajakontodega seotud poliitikarikkumisest.

4.1.4 Teostab järelevalvet poliitika läbivaatamiste, auditite ja rakendatavate meetmete üle.

4.2 IT-juht või väline IT-teenuse osutaja

4.2.1 Vastutab kontode ja õiguste kontrollimeetmete tehnilise rakendamise eest kõigis organisatsiooni kasutatavates süsteemides.

4.2.2 Loob, muudab ja deaktiveerib kasutajakontosid üksnes dokumenteeritud kinnituste alusel.

4.2.3 Rakendab paroolide keerukuse nõudeid, ekraaniluku ajalõppu, mitmikautentimist (kui see on saadaval) ja süsteemilogimist.

4.2.4 Säilitab turvalised kirjed kõigi juurdepääsukinnituste, konto omandi, õiguste eskaleerimiste ja tühistamiste kohta.

4.2.5 Seirab loata ning omaniku või kasutajata kontosid ning teatab lahknevustest tegevjuhile.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Käesoleva poliitika peavad tegevjuht ja IT-juht läbi vaatama vähemalt kord aastas, et tagada vastavus järgmisele:

9.1.1 Kehtivad ISO/IEC 27001:2022 kontrollimeetmed ja suunised

9.1.2 Regulatiivsed uuendused (nt GDPR, DORA, NIS2)

9.1.3 Muudatused süsteemides, teenustes või äristruktuuris

9.2 Läbivaatamine tuleb teha ka pärast järgmist:

9.2.1 Olulised turvaintsidendid või auditileiud

9.2.2 Olulised muudatused IT-süsteemides või kontode arhitektuuris

9.2.3 Uute platvormide kasutuselevõtt, mis nõuab juurdepääsukontrolli integreerimist

9.3 Kõik muudatused peab kinnitama tegevjuht ning need tuleb mõjutatud töötajatele selgelt teatavaks teha.

10. Seotud poliitikad ja seosed

10.1 P2S – Juhtimisrollide ja vastutuste poliitika: määratleb vastutuse ja otsustusõiguse juurdepääsu kinnitamisel ning järelevalves.

10.2 P4S – Juurdepääsukontrolli poliitika: reguleerib süsteemiülest juurdepääsukontrolli rakendamist ja autentimismeetodeid.

10.3 P7S – Töölevõtu ja töösuhte lõpetamise poliitika: tagab, et kontode loomine ja eemaldamine on seotud personali hallatavate töötajamuudatustega.

10.4 P8S – Infoturbeteadlikkuse ja koolituse poliitika: koolitab kasutajaid turvaliste kontohalduse tavade ja kasutusnõuete osas.

10.5 P30S – Intsidentidele reageerimise poliitika: määratleb tegevused, mida tuleb teha, kui konto väärkasutus põhjustab turvarikkumise või loata avalikustamise.

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 Punkt 5.3: nõuab, et infoturbe rollid ja vastutused oleksid selgelt määratletud ja rakendatud.

11.1.2 Punkt 8.1: operatiivne kavandamine ja kontroll peavad hõlmama kasutajate juurdepääsuhaldust.

11.2 ISO/IEC 27002

11.2.1 Kontroll 8.2: kirjeldab tehnilisi ja protseduurilisi kontrollimeetmeid kõrgendatud õiguste määramiseks, läbivaatamiseks ja eemaldamiseks.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: nõuab kontode loomist, seiret ja tühistamist määratletud rollide ja protsesside alusel.

11.3.2 AC-5: käsitleb tööülesannete lahusust, et vältida õiguste konflikti või kuritarvitust.

11.3.3 AC-6: nõuab vähimate õiguste põhimõtte rakendamist kõigile juurdepääsuõigustele.

11.4 EL GDPR

11.4.1 Artikkel 32: nõuab asjakohaseid juurdepääsukontrolle, et kaitsta isikuandmeid loata juurdepääsu või muutmise eest.

11.5 EL NIS

11.5.1 Artikkel 21(2)(d): nõuab kasutajate juurdepääsuhaldust elutähtsate ja oluliste üksuste peamiste turbekontrollide osana.

11.6 EL DORA

11.6.1 Artikkel 9(2)(b): nõuab, et finantssektori üksused rakendaksid juurdepääsukontrolle, mis piiravad ja seiravad privilegeeritud õigusi.

11.7 COBIT 2019

11.7.1 DSS05.03: määratleb kasutajate juurdepääsuõiguste andmise ja lõpetamise IT-juhtimise osana.

11.7.2 DSS05.04: nõuab kasutajate juurdepääsu pidevat läbivaatamist ja kooskõlastamist organisatsiooniliste rollidega.