					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P07					Dokumendi pealkiri: **Töölevõtu ja töösuhte lõpetamise 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 õigusnormidega

Standard/õigusnorm	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punkt 7.2, punkt 6	Personali pädevus, rolli turvaline integreerimine ning töösuhte lõpetamise või muudatustega seotud vastutuste rakendamine.
ISO/IEC 27002:2022	Kontrollimeetmed 6.2, 6.5, 5	Töölevõtu, juurdepääsu ja personali elutsükli kontrollimeetmed.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Personali üleviimine ja töösuhte lõpetamine, vähimate õiguste põhimõte, auditilogimine ning juurdepääsuhaldus personali muudatuste ajal ja järel.
ELi isikuandmete kaitse üldmäärus (GDPR)	Artiklid 5(1)(f), 25, 32; põhjendus 39	Juurdepääsu piiramine, konfidentsiaalsus, kaitse ning asjakohased kontrollimeetmed personaliandmete töötlemisel.
ELi NIS2	Artikkel 21(2)(b, c, d)	Personali- ja operatiivturbe meetmed, siseohtude maandamine ning elutsükli protsessid.
ELi DORA	Artiklid 5, 8, 9	Juhtimine, sisemine IKT-kontroll, IKT-riskide juhtimine ning intsidendihaldus personali ülemineku ajal.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Inimressursid, teadmusjuhtimine, turve ja vastavus töölevõtu ning töösuhte lõpetamise käigus.

1. Eesmärk

1.1 Käesolev poliitika kehtestab standarditud protseduurid sisseelamise, teisele ametikohale üleviimise ja töösuhte lõpetamise haldamiseks kõigi kasutajatüüpide lõikes.

1.2 See tagab füüsilise ja loogilise juurdepääsuõiguse õigeaegse ja turvalise andmise ning eemaldamise, rakendades samal ajal konfidentsiaalsust, aruandekohustust ja varade tagastamist.

1.3 Käesolev poliitika maandab volitamata juurdepääsu, andmelekkega ja tagastamata varadega seotud riske, lõimides sisseelamise ja lahkumisprotsessi kontrollimeetmed personali-, IT- ja turbeprotsessidesse.

1.4 See toetab standardi ISO/IEC 27001:2022 lisa A kontrolli 6.5 nõudeid, tagades, et personali turbekohustusi rakendatakse töösuhte või kaasamise ajal ja pärast selle lõppu.

2. Kohaldamisala

2.1 Käesolev poliitika kohaldub kõigile töötajatele, töövõtjatele, konsultantidele, tarnijatele ja teistele kolmandatele isikutele, kellele on antud juurdepääs organisatsiooni süsteemidele, võrkudele, rajatistele või andmetele.

2.2 See reguleerib järgmiste tegevuste täielikku elutsüklit:

2.2.1 sisseelamine (värbamine, lepinguline kaasamine või ajutine kaasamine)

2.2.2 teisele ametikohale üleviimine või rollimuudatused

2.2.3 lahkumisprotsess (lahkumisavaldus, pensionile jäämine, töösuhte lõpetamine, lepingu lõppemine)

2.3 Poliitika hõlmab:

2.3.1 loogilist juurdepääsu (süsteemid, rakendused, pilveteenused, VPN)

2.3.2 füüsilist juurdepääsu (pääsukaardid, võtmed, hoonesse sisenemise süsteemid)

2.3.3 määratud varasid (sülearvutid, telefonid, tokenid, autentimisandmed)

2.3.4 poliitikatega tutvumise kinnitamist ja konfidentsiaalsuskohustusi

2.4 Kõik osakonnad (personal, IT, rajatiste ja varade haldus, turve ja juhtkond) vastutavad oma rolli täitmise eest sisseelamise ja lahkumisprotsessi töövoogudes.

3. Eesmärgid

3.1 Tagada, et kõigile töötajatele ja seotud isikutele antakse juurdepääs alles pärast turbe-, koolitus- ja lepinguliste eeltingimuste täitmist.

3.2 Tühistada juurdepääsuõigused ja tagastada organisatsiooni varad viivitamata rollimuudatuse või töösuhte lõpetamise korral.

3.3 Säilitada organisatsiooni varade konfidentsiaalsus, terviklus ja käideldavus personali üleminekute ajal.

3.4 Toetada auditivalmidust ja õiguslikku kaitstavust sisseelamise ja töösuhte lõpetamise sündmuste täielike kirjete kaudu.

3.5 Vähendada siseohtude riski, valideerides ja dokumenteerides kõik personaliga seotud juurdepääsusündmused.

3.6 Viia organisatsiooni personali elutsükkel kooskõlla riskipõhiste turbepraktikate ja regulatiivsete nõuetega.

4. Rollid ja vastutused

4.1 Tippjuhtkond

4.1.1 Kiidab käesoleva poliitika heaks ning eraldab volitused ja ressursid sisseelamise, lahkumisprotsessi ja pääsukontrolli protsesside jaoks.

4.1.2 Tagab, et personali üleminekud ei seaks organisatsiooni põhjendamatu turbe- ega õigusliku riski alla.

4.2 Personaliosakond

4.2.1 Algatab töötajate töölevõtu ja töösuhte lõpetamise töövood ning teavitab asjakohaseid osakondi muudatustest.

4.2.2 Tagab, et taustakontrollid, lepingud, konfidentsiaalsuslepingud (NDA) ja poliitikatega tutvumise kinnitused on enne juurdepääsu andmist lõpule viidud.

4.2.3 Teavitab IT-d ja rajatiste haldust töötajate lahkumisest kooskõlas teavitamise SLA-ga.

4.2.4 Koordineerib õigus- ja vastavusfunktsiooniga töösuhtejärgsete kohustuste rakendamist (nt konfidentsiaalsusklauslid).

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 Poliitika läbivaatamise sagedus

9.1.1 Käesolev poliitika tuleb läbi vaadata:

9.1.1.1 kord aastas või

9.1.1.2 pärast mis tahes olulist intsidenti, mis hõlmab juurdepääsu väärkasutust, varade kaotust või protseduurilist tõrget

9.1.1.3 suuremate HR- või IAM-platvormi muudatuste rakendamisel

9.1.1.4 personaliandmeid või kohustusi mõjutavate õiguslike või regulatiivsete muudatuste korral

9.2 Läbivaatamise protsess ja vastutus

9.2.1 ISMS-i juht ja personalidirektor koordineerivad läbivaatamist IT-turbe ning õigus- ja vastavusfunktsiooni sisendi alusel.

9.2.2 Kõik muudatused peab heaks kiitma tippjuhtkond ja infoturbe juhtimissüsteemi juhtkomitee.

9.2.3 Muudetud versioonid tuleb mõjutatud osakondadele ja töötajatele uuesti kinnitamiseks edastada.

9.3 Dokumendiohje ja säilitamine

9.3.1 Käesolev poliitika peab sisaldama:

9.3.2 versioonihaldust, muudatuste ajalugu ja jõustumiskuupäeva

9.3.3 vastutavat omanikku ja läbivaatajaid

9.3.4 poliitika klassifikatsiooni ja heakskiidukirjet

9.3.5 Kehtetud versioonid tuleb dokumendihalduse poliitika kohaselt arhiveerida vähemalt 3 aastaks.

10. Seotud poliitikad ja seosed

10.1.1 Käesolev poliitika on otseselt seotud järgmiste dokumentidega:

10.1.2 P1 – Infoturbepoliitika: määratleb organisatsiooni turbe-eesmärgid, sealhulgas personali juurdepääsu juhtimise.

10.1.3 P4 – Juurdepääsukontrolli poliitika: sätestab töölevõtu ja töösuhte lõpetamise käivitusel põhinevad süsteemi- ja füüsilise juurdepääsu andmise ning tühistamise tegevusnõuded.

10.1.4 P3 – Lubatud kasutuse poliitika: nõuab töölevõtu käigus tutvumise kinnitamist ja toetab poliitika järgimist pärast töösuhte lõppu.

10.1.5 P6 – Riskijuhtimise poliitika: tagab, et kasutaja juurdepääsu ja üleminekutega seotud riske hinnatakse ning maandatakse kooskõlas ISMS-i põhimõtetega.

10.1.6 P11 – Kasutajakontode ja privileegide haldamise poliitika: reguleerib käesoleva poliitika toetuseks juurdepääsuõiguste andmise ja eemaldamise tehnilisi kontrollimeetmeid.

10.2 Need poliitikad moodustavad inimeste elutsükli sündmuste turvaliseks ja aruandekohustuslikuks haldamiseks lõimitud kontrollisüsteemi.

11. Viitestandardid ja raamistikud

11.1 Käesolev poliitika on kooskõlas rahvusvaheliselt tunnustatud turbe-, andmekaitse- ja IT-juhtimise raamistikega, et tagada töölevõtu ja töösuhte lõpetamise protsesside turvalisus, jälgitavus ja vastavus õiguslikele ning organisatsioonilistele nõuetele.

11.2 ISO/IEC 27001:

11.2.1 Punkt 7.2 – pädevus ja punkt 6.2 – infoturbe eesmärgid: käesolev poliitika toetab personali pädevuse kujundamist ja isikute turvalist integreerimist rollidesse, kus nad mõjutavad ISMS-i eesmärke.

11.2.2 Lisa A kontroll 6.5 – kohustused pärast töösuhte lõpetamist või muutmist: käesolev poliitika rakendab täielikult kontrollimeetmeid, mis käsitlevad jääkjuurdepääsuõigusi, andmete valdust ja lepingulisi kohustusi lahkumise korral.

11.2.3 Lisa A kontroll 5.9 – taustakontroll ja 6.2 – töösuhte tingimused: töölevõtu protseduurid sisaldavad taustakontrolli ja poliitikatega tutvumise kinnitamise mehhanisme kooskõlas nende punktidega.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (personali töösuhte lõpetamine) ja PS-5 (personali üleviimine): käesolev poliitika rakendab juurdepääsuõiguste, füüsiliste pääsukaartide ja varade struktureeritud eemaldamist või muutmist.

11.3.2 AC-2 (kontohaldus) ja AC-6 (vähimate õiguste põhimõte): sätted tagavad, et juurdepääs on rolliga kooskõlas ja tühistatakse viivitamata, kui see ei ole enam vajalik.

11.3.3 IA-4 (identifikaatorite haldus) ja IA-5 (autentijate haldus): toetab autentimisandmete turvalist haldamist personali muudatuste ajal ja järel.

11.3.4 CM-5 (muudatuste juurdepääsupiirangud): hoiab ära volitamata muudatused pärast töösuhte lõppu privilegeeritud juurdepääsuõiguste tühistamise kaudu.

11.3.5 AU-2 ja AU-6: juurdepääsusündmuste logimist ja jälgitavust tugevdatakse IAM-i ning auditijälje lõimimise kaudu.

11.4 ELi isikuandmete kaitse üldmäärus (GDPR) (2016/679):

11.4.1 Artikkel 5(1)(f): kaitseb isikuandmeid volitamata juurdepääsu eest, mida käesolev poliitika rakendab kasutaja juurdepääsu tühistamisega lahkumisprotsessi käigus.

11.4.2 Artikkel 32: nõuab asjakohaseid tehnilisi ja korralduslikke meetmeid isikuandmete kaitseks kogu töösuhte elutsükli jooksul.

11.4.3 Artikkel 25 – lõimitud andmekaitse: tagab, et töölevõtt ja töösuhte lõpetamine hõlmavad andmete minimeerimist, säilitamist ja õiguspärase juurdepääsu kontrollimeetmeid.

11.4.4 Põhjendus 39: rõhutab juurdepääsu piiramist ja konfidentsiaalsust, mida toetab käesoleva poliitika ülesehitus.

11.5 ELi NIS2 direktiiv (2022/2555):

11.5.1 Artikkel 21(2)(b, c, d): nõuab personali- ja operatiivturbe meetmeid pääsukontrolli, siseohtude maandamise ja elutsükli protsesside käsitlemiseks, mis kõik kajastuvad käesolevas poliitikas.

11.6 ELi DORA (2022/2554):

11.6.1 Artikkel 5 – juhtimine ja sisekontroll: käesolev poliitika toetab inimriskide ja juurdepääsuhaldusega seotud sisemist IKT-juhtimist.

11.6.2 Artikkel 8 – IKT-riskide juhtimine: rakendab kontrollimeetmeid personali üleminekutele, mis võivad seada ohtu kriitilised varad või reguleeritud keskkonnad.

11.6.3 Artikkel 9 – intsidentide klassifitseerimine ja haldus: tagab, et töösuhte lõpetamisega seotud rikkumised on teatatavad ja maandatud nõuetekohase juurdepääsuõiguste eemaldamise ning varade käsitlemise kaudu.

11.7 COBIT 2019:

11.7.1 APO07 – hallatud inimressursid: määratleb töölevõtu ja töösuhte lõpetamise rollid, vastutused ja elutsükli tegevused kooskõlas juhtimise eesmärkidega.

11.7.2 BAI08 – teadmusjuhtimine: tugevdab protseduuride dokumenteerimist, teadmiste säilitamist ja kontrolli üleandmist töösuhte lõppemisel.

11.7.3 DSS05 – hallatud turvateenused: rakendab kasutajate deaktiveerimist, varade kontrolli ja aruandekohustust rollimuudatuste ajal.

11.7.4 MEA03 – vastavuse seire, hindamine ja auditeerimine: tagab, et sisseelamise ja lahkumisprotsessi kontrollimeetmeid hinnatakse sise- ja välisauditite käigus.