					Sisestage siia registreeritud juriidilise isiku nimi							
Dokumendi number: P07S					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**

Kooskõlas standardite ja regulatsioonidega

Standard/õigusakt	Punkt/artikkel	Kommentaar
ISO/IEC 27001:2022	Punktid 6.2, 7	Personaliturbe ja teadlikkuse nõuded
ISO/IEC 27002:2022	Kontrollimeetmed 6.2, 6.5	Töölevõtu ja töösuhte lõpetamise turbepraktikad
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Töösuhte lõpetamine, kontode elutsükkel, planeerimine
EL NIS2	Artikkel 21(2)(h)	Personaliturve ja juurdepääsu elutsükkel
EL DORA	Artikkel 12	Juurdepääsukontrollid ja õiguste tühistamine IKT-süsteemides
COBIT 2019	APO07, DSS01	Personaliturve, loogilise ja füüsilise juurdepääsu kontrollid
EL isikuandmete kaitse üldmäärus (GDPR)	Artikkel 32	Isikuandmete turve töösuhte ajal

1. Eesmärk

1.1 Käesolev poliitika määratleb uute töötajate ja töövõtjate töölevõtmise protsessi ning juurdepääsu turvalise lõpetamise, kui isik lahkub organisatsioonist või vahetab rolli.

1.2 Poliitika tagab, et juurdepääsuõigusi antakse üksnes vajaduspõhiselt ja vähimate õiguste põhimõtte alusel, kõik varad on arvele võetud ning kriitilised tegevused, nagu süsteemide deaktiveerimine ja andmete üleandmine või taastamine, viiakse ellu viivitamata.

1.3 Käesolev poliitika toetab vastavust, tööprotsesside terviklust ja andmekaitset struktureeritud ning auditeeritavate töölevõtu ja töösuhte lõpetamise tegevuste kaudu.

2. Kohaldamisala

2.1 Käesolev poliitika kehtib järgmiste isikute suhtes:

2.1.1 kõik alalised ja ajutised töötajad

2.1.2 töövõtjad, konsultandid ja praktikandid

2.1.3 välised teenuseosutajad, kellel on süsteemi- või füüsiline juurdepääs

2.2 Poliitika hõlmab järgmist:

2.2.1 töölevõtmise protsess: kasutajakontode loomine, juurdepääsuõiguste andmine, seadmete väljastamine

2.2.2 lahkumisprotsess: juurdepääsuõiguste eemaldamine, ettevõtte varade tagastamine ja digitaalsete identiteetide turvaline sulgemine

2.2.3 ettevõttesisesed rollimuudatused, mis nõuavad juurdepääsuõiguste ümberseadistamist või varade ümbermääramist

2.3 Käesolev poliitika kehtib kõigile seadmetele, platvormidele ja asukohtadele, mida kasutatakse ametiülesannete täitmiseks.

3. Eesmärgid

3.1 Tagada, et uued töötajad saavad juurdepääsu ja ressursid kontrollitud rollide ning vastutuste alusel.

3.2 Tagada, et lahkuvate kasutajate juurdepääs süsteemidele ja ruumidele eemaldatakse täielikult hiljemalt nende viimasel tööpäeval.

3.3 Ennetada omanikuta kasutajakontosid ja tagastamata varasid, mis kujutavad endast turberiski.

3.4 Tagada dokumenteeritud kirjed töölevõtmise, üleviimiste ja lahkumisprotsessi tegevuste kohta.

3.5 Tugevdada aruandekohustust kontrollnimekirjade ja valdkondadeülese rollikoordineerimise kaudu.

4. Rollid ja vastutused

4.1 tegevjuht

4.1.1 kiidab heaks kõrgendatud juurdepääsuõigustega rollide juurdepääsu ning teostab järelevalvet töölevõtmise ja töösuhte lõpetamise protsessi üle.

4.1.2 tagab, et erandid on põhjendatud ja protsesside mittejärgimise korral rakendatakse parandusmeetmeid.

4.2 büroojuht / personalijuhtimine (HR)

4.2.1 algatab uute töötajate töölevõtmise protsessi ja teavitab IT-d lahkumistest.

4.2.2 tagab õigusdokumentide, näiteks konfidentsiaalsuslepingu (NDA), ning poliitikaga tutvumise kinnituste vormistamise.

4.2.3 haldab tööleasumise ja töölt lahkumise kontrollnimekirju ning jälgib poliitika järgimist.

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

9. Läbivaatamise ja ajakohastamise nõuded

9.1 iga-aastane läbivaatamine

9.1.1 käesolev poliitika tuleb vähemalt kord aastas läbi vaadata tegevjuhi ning HR- ja IT-vastutajate poolt.

9.2 varajase läbivaatamise käivitajad

9.2.1 ajakohastamine tuleb teha, kui:

9.2.1.1 võetakse kasutusele uued HR- või IT-süsteemid

9.2.1.2 muutub väline IT-teenuse osutaja või hallatav HR-teenus

9.2.1.3 turvaauditid tuvastavad protsessilüngad

9.2.1.4 regulatiivsed kohustused muutuvad, näiteks GDPR-i uuenduste tõttu

9.2.1.5 toimub kriitiline lahkumisprotsessi ebaõnnestumine või rikkumine

9.3 versioonihaldus ja heakskiitmine

9.3.1 käesoleva poliitika iga versioon peab sisaldama järgmist:

9.3.1.1 versiooninumber ja kuupäev

9.3.1.2 muudatuste kokkuvõte

9.3.1.3 tegevjuhi heakskiit

9.3.1.4 arhiveeritud varasemaid versioone tuleb säilitada vähemalt kolm aastat

9.4 teavitamine ja kinnitamine

9.4.1 kõiki töötajaid, kes vastutavad töölevõtmise või töösuhte lõpetamise eest, tuleb teavitada kõigist poliitikamuudatustest. Iga-aastased teadlikkuse tõstmise või korduskoolituse briifingud on kohustuslikud.

10. Seotud poliitikad ja seosed

10.1 Käesolev poliitika toetab järgmisi poliitikaid ja on nendega seotud:

10.1.1 P2S – Juhtimisrollide ja vastutuste poliitika: tagab aruandekohustuse juurdepääsu ja töölevõtmise protsessi korraldamisel

10.1.2 P4S – Juurdepääsukontrolli poliitika: määratleb rollipõhise juurdepääsuõiguste andmise ja deaktiveerimise tehnilise rakendamise

10.1.3 P6S – Riskijuhtimise poliitika: hindab riske, mis tulenevad töölevõtmise ja töösuhte lõpetamise kontrollimeetmete tõrgetest

10.1.4 P8S – Infoturbeteadlikkuse koolituse poliitika: kehtestab töötajate sisseelamise nõuded tööleasumisel

10.1.5 P30S – Intsidentidele reageerimise poliitika: käsitleb juurdepääsuõiguste eemaldamata jätmist või varade vargust turvaintsidentidena

11. Viitestandardid ja raamistikud

11.1 ISO/IEC 27001

11.1.1 punkt 6.2 – kehtestab personaliturbe nõuded

11.1.2 punkt 7.2 – nõuab uutele töötajatele teadlikkuse koolitust

11.2 ISO/IEC 27002

11.2.1 kontrollimeetmed 6.2 ja 6.5 – kirjeldavad töölevõtmise ja töösuhte lõpetamise turbepraktikaid

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – töösuhte lõpetamise protseduurid, sealhulgas juurdepääsu deaktiveerimine

11.3.2 AC-2 – tagab kasutajakontode elutsükli halduse

11.3.3 PL-4 – nõuab personali üleminekute planeerimist

11.4 EL isikuandmete kaitse üldmäärus (GDPR)

11.4.1 artikkel 32 – tagab asjakohase turbe töösuhte ajal ja pärast seda, eelkõige isikuandmetele juurdepääsu korral

11.5 EL NIS2 direktiiv

11.5.1 artikkel 21(2)(h) – nõuab personaliturvet ja juurdepääsu elutsükli kontrollimeetmeid

11.6 EL DORA

11.6.1 artikkel 12 – nõuab reguleeritud finantsüksustelt töötajate juurdepääsu kontrolli IKT-süsteemidele, sealhulgas õiguste tühistamise protseduure

11.7 COBIT 2019

11.7.1 APO07 – personali juhtimine: kehtestab personali elutsükli turbenõuded

11.7.2 DSS01 – operatsioonide juhtimine: hõlmab loogilise ja füüsilise juurdepääsu kontrolli töösuhte üleminekute ajal