					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P07S					Dokumenta nosaukums: **Darba attiecību uzsākšanas un izbeigšanas politika**							
Versija: 1.0		Spēkā stāšanās datums: 01.01.2025			Dokumenta īpašnieks:							
X	Politika		Standarts		Procedūra		Veidlapa		Reģistrs		Cits	

Pārskatījumu vēsture				
Pārskatījuma numurs	**Pārskatījuma datums**	**Izmaiņas**	**Pārskatīja**	**Procesa īpašnieks**

Apstiprinājumi			
Vārds	**Amats**	**Datums**	**Paraksts**

Juridiskais paziņojums (autortiesības un lietošanas ierobežojumi)
(C) 2025 Clarysec LLC. All rights reserved.

Šis dokuments ir Clarysec LLC intelektuālais īpašums. Nevienu šī dokumenta daļu nedrīkst kopēt, atkārtoti izmantot, izplatīt vai grozīt komerciāliem vai ieviešanas nolūkiem bez iepriekšējas skaidras rakstiskas atļaujas.
Neautorizēta lietošana ir stingri aizliegta un var izraisīt tiesvedību.
Par licencēšanu sazinieties: info@clarysec.com

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkti 6.2, 7	Cilvēkresursu drošības un informētības prasības
ISO/IEC 27002:2022	Kontroles pasākumi 6.2, 6.5	Darba attiecību uzsākšanas un izbeigšanas drošības prakse
NIST SP 800-53 Rev.5	PS-4, AC-2, PL-4	Darba attiecību izbeigšana; piekļuves dzīves cikla pārvaldība; plānošana
ES NIS2	21. pants (2)(h)	Cilvēkresursu drošība un piekļuves dzīves cikls
ES DORA	12. pants	Piekļuves kontrole un atsaukšana IKT sistēmām
COBIT 2019	APO07, DSS01	Personāla drošība, loģiskās un fiziskās piekļuves kontroles pasākumi
ES GDPR	32. pants	Personas datu drošība nodarbinātības laikā

1. Mērķis

1.1 Šī politika nosaka jaunu darbinieku un līgumslēdzēju uzņemšanas procesu un drošu piekļuves atsaukšanu, personām izbeidzot darba attiecības vai mainot amatu.

1.2 Tā nodrošina, ka piekļuves tiesības tiek piešķirtas atbilstoši minimālo privilēģiju principam, visi aktīvi tiek uzskaitīti un kritiski svarīgas darbības, piemēram, sistēmu deaktivizēšana un datu atjaunošana, tiek veiktas savlaicīgi.

1.3 Šī politika atbalsta atbilstību, darbības integritāti un datu aizsardzību, nosakot strukturētas un auditējamas uzņemšanas un darba attiecību izbeigšanas procesa darbības.

2. Tvērums

2.1 Šī politika attiecas uz:

2.1.1 visiem pastāvīgajiem un pagaidu darbiniekiem;

2.1.2 līgumslēdzējiem, konsultantiem un praktikantiem;

2.1.3 ārējiem pakalpojumu sniedzējiem, kuriem ir sistēmu vai fiziskā piekļuve.

2.2 Tā aptver:

2.2.1 uzņemšanu: lietotāju kontu izveidi, piekļuves tiesību piešķiršanu, aprīkojuma izsniegšanu;

2.2.2 darba attiecību izbeigšanas procesu: piekļuves tiesību atsaukšanu, uzņēmuma aktīvu atgūšanu un digitālo identitāšu drošu slēgšanu;

2.2.3 iekšējās amata izmaiņas, kurām nepieciešama piekļuves pārkonfigurēšana vai aktīvu pārpiešķiršana.

2.3 Tā ir piemērojama visām ierīcēm, platformām un atrašanās vietām, kas tiek izmantotas oficiālo darba pienākumu veikšanai.

3. Mērķi

3.1 Nodrošināt, ka jaunie darbinieki saņem piekļuves tiesības un resursus, pamatojoties uz pārbaudītām lomām un pienākumiem.

3.2 Nodrošināt, ka aizejošo lietotāju piekļuve sistēmām un telpām tiek pilnībā atsaukta līdz viņu pēdējās darba dienas beigām.

3.3 Novērst bezsaimnieka kontus un neatdotus aktīvus, kas rada drošības risku.

3.4 Uzturēt dokumentētus ierakstus par uzņemšanas, amata maiņas un darba attiecību izbeigšanas procesa darbībām.

3.5 Veicināt pārskatatbildību, izmantojot kontrolsarakstus un starpfunkcionālu lomu koordināciju.

4. Lomas un atbildība

4.1 Ģenerāldirektors

4.1.1 Apstiprina piekļuves tiesības augsti privileģētām lomām un uzrauga darba attiecību uzsākšanas un izbeigšanas programmu.

4.1.2 Nodrošina, ka izņēmumi ir pamatoti un tiek veiktas koriģējošās darbības, ja procesi netiek ievēroti.

4.2 Biroja vadītājs / cilvēkresursu funkcija (HR)

4.2.1 Uzsāk uzņemšanas procesu jaunajiem darbiniekiem un informē IT par darba attiecību izbeigšanu.

4.2.2 Nodrošina juridisko dokumentu noformēšanu (piemēram, konfidencialitātes līgumu) un politikas iepazīšanās apliecinājumu saņemšanu.

4.2.3 Uztur uzņemšanas un izbeigšanas kontrolsarakstus un uzrauga politikas ievērošanu.

[... Sadaļas 4.3–8 nav iekļautas šajā priekšskatījumā. Iegādājieties pilnu dokumentu, lai piekļūtu pilnam saturam. ...]

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ikgadējā pārskatīšana

9.1.1 Šī politika jāpārskata vismaz reizi gadā ģenerāldirektoram un HR/IT vadītājiem.

9.2 Priekšlaicīgas pārskatīšanas ierosinātāji

9.2.1 Atjauninājumi jāveic, ja:

9.2.1.1 tiek ieviestas jaunas HR vai IT sistēmas;

9.2.1.2 mainās ārējais IT pakalpojumu sniedzējs vai pārvaldīts HR pakalpojums;

9.2.1.3 drošības auditos tiek konstatēti procesu trūkumi;

9.2.1.4 mainās regulatīvās prasības (piemēram, GDPR atjauninājumi);

9.2.1.5 notiek kritiska darba attiecību izbeigšanas procesa kļūme vai pārkāpums.

9.3 Versiju kontrole un apstiprināšana

9.3.1 Katrā šīs politikas versijā jāiekļauj:

9.3.1.1 versijas numurs un datums;

9.3.1.2 izmaiņu kopsavilkums;

9.3.1.3 ģenerāldirektora apstiprinājums;

9.3.1.4 arhivētas iepriekšējās versijas, kas jāglabā vismaz trīs gadus.

9.4 Komunikācija un apliecinājums

9.4.1 Visi darbinieki, kuri ir atbildīgi par uzņemšanu vai darba attiecību izbeigšanu, jāinformē par jebkādiem politikas atjauninājumiem. Ikgadējā informētība vai atkārtota instruktāža ir obligāta.

10. Saistītās politikas un sasaistes

10.1 Šī politika atbalsta un to papildina šādas politikas:

10.1.1 P2S – Pārvaldības lomu un atbildības politika: nodrošina pārskatatbildību piekļuves un uzņemšanas procesos.

10.1.2 P4S – Piekļuves kontroles politika: nosaka tehnisko ieviešanu lomu balstītai piekļuves tiesību piešķiršanai un deaktivizēšanai.

10.1.3 P6S – Risku pārvaldības politika: izvērtē riskus, kas izriet no uzņemšanas un darba attiecību izbeigšanas kontroles pasākumu nepilnībām.

10.1.4 P8S – Informācijas drošības informētības un apmācības politika: nosaka personāla ievadinstruktāžas prasības uzņemšanas laikā.

10.1.5 P30S – Incidentu reaģēšanas politika: piekļuves tiesību neatsaukšanu vai aktīvu zādzību traktē kā drošības incidentus.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 Punkts 6.2 – nosaka cilvēkresursu drošības prasības.

11.1.2 Punkts 7.2 – nosaka obligātas informētības apmācības prasības jaunajiem darbiniekiem.

11.2 ISO/IEC 27002

11.2.1 Kontroles pasākumi 6.2 un 6.5 – detalizē darba attiecību uzsākšanas un izbeigšanas drošības praksi.

11.3 NIST SP 800-53 Rev. 5

11.3.1 PS-4 – darba attiecību izbeigšanas procedūras, tostarp piekļuves deaktivizēšana.

11.3.2 AC-2 – nodrošina lietotāju piekļuves dzīves cikla pārvaldību.

11.3.3 PL-4 – nosaka prasību plānot personāla pārejas.

11.4 ES GDPR

11.4.1 32. pants – nodrošina atbilstošu drošību nodarbinātības laikā un pēc tās, īpaši attiecībā uz piekļuvi personas datiem.

11.5 ES NIS2 direktīva

11.5.1 21. pants (2)(h) – nosaka cilvēkresursu drošības un piekļuves dzīves cikla kontroles pasākumus.

11.6 ES DORA

11.6.1 12. pants – nosaka prasību regulētām finanšu iestādēm kontrolēt personāla piekļuvi IKT sistēmām, tostarp atsaukšanas procedūras.

11.7 COBIT 2019

11.7.1 APO07 – cilvēkresursu pārvaldība: nosaka personāla dzīves cikla drošības prasības.

11.7.2 DSS01 – operāciju pārvaldība: aptver loģiskās un fiziskās piekļuves kontroles pasākumus darba attiecību pārejas laikā.