					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P07					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**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	7. punkts, 6. punkts	Personāla kompetence, droša integrēšana un pienākumu ievērošana darba attiecību izbeigšanas vai maiņas gadījumā.
ISO/IEC 27002:2022	6.2., 6.5., 5. kontroles pasākumi	Ievadīšanas process, piekļuve un personāla dzīves cikla kontroles pasākumi.
NIST SP 800-53 Rev.5	PS-4, PS-5, AC-2, AC-6, IA-4, IA-5, CM-5, AU-2, AU-6	Personāla pārcelšana un darba attiecību izbeigšana, minimālo privilēģiju princips, audita žurnālfiksēšana, piekļuves pārvaldība personāla izmaiņu laikā un pēc tām.
EU GDPR	5(1)(f), 25., 32. pants; 39. apsvērums	Piekļuves ierobežošana, konfidencialitāte, aizsardzība un atbilstoši kontroles pasākumi personāla datiem.
EU NIS2	21. panta 2. punkta b), c), d) apakšpunkts	Personāla un operacionālās drošības pasākumi; iekšējo apdraudējumu mazināšana; dzīves cikla procesi.
EU DORA	5., 8., 9. pants	Pārvaldība, iekšējā IKT kontrole, IKT risks, incidentu pārvaldība personāla pārejas laikā.
COBIT 2019	APO07, BAI08, DSS05, MEA03	Cilvēkresursi, zināšanu pārvaldība, drošība un atbilstība darba attiecību uzsākšanas un izbeigšanas procesā.

1. Mērķis

1.1 Šī politika nosaka standartizētas procedūras ievadīšanas, iekšējās pārcelšanas un darba attiecību izbeigšanas pārvaldībai visiem lietotāju veidiem.

1.2 Tā nodrošina savlaicīgu un drošu fiziskās un loģiskās piekļuves piešķiršanu un piekļuves tiesību atsaukšanu, vienlaikus nodrošinot konfidencialitāti, pārskatatbildību un aktīvu atgūšanu.

1.3 Šī politika mazina riskus, kas saistīti ar nesankcionētu piekļuvi, datu noplūdi un neatgrieztiem aktīviem, integrējot darba attiecību uzsākšanas un izbeigšanas kontroles pasākumus cilvēkresursu, IT un drošības procesos.

1.4 Tā atbalsta ISO/IEC 27001:2022 A pielikuma 6. kontroles pasākumu 6.5, nodrošinot, ka personāla drošības pienākumi tiek ievēroti darba vai sadarbības laikā un pēc tās.

2. Tvērums

2.1 Šī politika attiecas uz visiem darbiniekiem, līgumdarbiniekiem, trešo personu pakalpojumu sniedzējiem, konsultantiem, piegādātājiem un citām trešajām personām, kurām ir piešķirta piekļuve organizācijas sistēmām, tīkliem, telpām vai datiem.

2.2 Tā reglamentē pilnu dzīves ciklu attiecībā uz:

2.2.1 ievadīšanas procesu (pieņemšana darbā, līguma noslēgšana vai pagaidu iesaiste)

2.2.2 iekšējo pārcelšanu vai lomas maiņu

2.2.3 darbinieka aiziešanas procesu (atkāpšanās no amata, ekspluatācijas pārtraukšana, darba attiecību izbeigšana, līguma termiņa beigas)

2.3 Politika aptver:

2.3.1 loģisko piekļuvi (sistēmas, lietojumprogrammas, mākoņpakalpojumi, uzņēmuma VPN)

2.3.2 fizisko piekļuvi (piekļuves kartes, atslēgas, ēkas piekļuves sistēmas)

2.3.3 piešķirtos aktīvus (portatīvie datori, tālruņi, marķieri, pieteikšanās dati)

2.3.4 politikas apliecināšanu un konfidencialitātes pienākumus

2.4 Visas struktūrvienības (cilvēkresursi, IT, objektu un aktīvu pārvaldība, drošība un vadība) ir atbildīgas par savas lomas izpildi darba attiecību uzsākšanas un izbeigšanas darbplūsmās.

3. Mērķi

3.1 Nodrošināt, ka visam personālam piekļuve tiek piešķirta tikai pēc drošības, apmācību un līgumisko priekšnoteikumu izpildes.

3.2 Atsaukt piekļuves tiesības un atgūt organizācijas aktīvus nekavējoties pēc lomas maiņas vai darba attiecību izbeigšanas.

3.3 Saglabāt organizācijas aktīvu konfidencialitāti, integritāti un pieejamību personāla pārejas laikā.

3.4 Atbalstīt auditējamību un tiesisko aizsargājamību, nodrošinot pilnīgus ierakstus par darba attiecību uzsākšanas un izbeigšanas notikumiem.

3.5 Samazināt pakļautību iekšējiem apdraudējumiem, validējot un dokumentējot visus ar personālu saistītos piekļuves notikumus.

3.6 Saskaņot organizācijas personāla dzīves ciklu ar uz risku balstītu lēmumu pieņemšanu drošības praksē un normatīvajiem pienākumiem.

4. Lomas un atbildība

4.1 Izpildvadība

4.1.1 Apstiprina šo politiku un piešķir pilnvaras un resursus darba attiecību uzsākšanas, darbinieka aiziešanas un piekļuves kontroles procesiem.

4.1.2 Nodrošina, ka personāla pārejas nerada organizācijai nepamatotu drošības vai juridisko risku.

4.2 Cilvēkresursi

4.2.1 Uzsāk ievadīšanas un darba attiecību izbeigšanas darbplūsmas darbiniekiem un informē attiecīgās struktūrvienības par izmaiņām.

4.2.2 Nodrošina, ka fona pārbaudes, līgumi, konfidencialitātes līgumi un politikas iepazīšanās apliecinājumi ir pabeigti pirms piekļuves piešķiršanas.

4.2.3 Informē IT un objektu un aktīvu pārvaldību par darbinieku aiziešanu saskaņā ar paziņošanas pakalpojumu līmeņa vienošanos.

4.2.4 Koordinējas ar juridisko un atbilstības funkciju, lai nodrošinātu pēcdarba attiecību pienākumu izpildi (piemēram, konfidencialitātes klauzulas).

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Politikas pārskatīšanas biežums

9.1.1 Šī politika jāpārskata:

9.1.1.1 katru gadu; vai

9.1.1.2 pēc jebkura būtiska incidenta, kas saistīts ar piekļuves ļaunprātīgu izmantošanu, aktīvu zaudējumu vai procesuālu kļūmi;

9.1.1.3 ieviešot būtiskas HR vai IAM platformas izmaiņas;

9.1.1.4 pēc normatīvo vai juridisko prasību izmaiņām, kas ietekmē personāla datus vai pienākumus.

9.2 Pārskatīšanas process un atbildība

9.2.1 Informācijas drošības pārvaldības sistēmas vadītājs un HR direktors koordinē pārskatīšanu, iesaistot IT drošību, juridisko un atbilstības funkciju.

9.2.2 Visas izmaiņas jāapstiprina izpildvadībai un Informācijas drošības vadības komitejai (ISSC).

9.2.3 Pārskatītās versijas atkārtoti jāizplata skartajām struktūrvienībām un personālam atkārtotai iepazīšanās apliecināšanai.

9.3 Dokumentu kontrole un glabāšana

9.3.1 Šai politikai jāietver:

9.3.2 versiju kontrole, izmaiņu vēsture un spēkā stāšanās datums;

9.3.3 atbildīgais īpašnieks un pārskatītājs(-i);

9.3.4 politikas klasifikācija un apstiprinājuma ieraksts.

9.3.5 Novecojušās versijas jāarhivē vismaz 3 gadus saskaņā ar dokumentu pārvaldības politiku.

10. Saistītās politikas un sasaistes

10.1.1 Šī politika ir tieši sasaistīta ar:

10.1.2 P1 – Informācijas drošības politika: nosaka organizācijas drošības mērķus, tostarp personāla piekļuves pārvaldību.

10.1.3 P4 – Piekļuves kontroles politika: nosaka darbības prasības sistēmu un fiziskās piekļuves piešķiršanai un atsaukšanai, pamatojoties uz darba attiecību uzsākšanas un izbeigšanas trigeriem.

10.1.4 P3 – Pieļaujamās lietošanas politika: paredz iepazīšanās apliecinājumu darba attiecību uzsākšanas laikā un atbalsta ievērošanu pēc darba attiecību izbeigšanas.

10.1.5 P6 – Risku pārvaldības politika: nodrošina, ka lietotāju piekļuves un pārejas riski tiek izvērtēti un mazināti saskaņā ar ISMS principiem.

10.1.6 P11 – Lietotāju kontu un privilēģiju pārvaldības politika: reglamentē tehniskos kontroles pasākumus piekļuves piešķiršanai un piekļuves tiesību atsaukšanai šīs politikas atbalstam.

10.2 Šīs politikas veido integrētu kontroles sistēmu, lai personāla dzīves cikla notikumi tiktu pārvaldīti droši un ar pārskatatbildību.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiski atzītiem drošības, privātuma un IT pārvaldības ietvariem, lai nodrošinātu, ka darba attiecību uzsākšanas un izbeigšanas procesi ir droši, izsekojami un atbilst tiesiskajām un organizācijas prasībām.

11.2 ISO/IEC 27001:

11.2.1 7.2. punkts – kompetence un 6.2. punkts – informācijas drošības mērķi: šī politika atbalsta personāla kompetences nodrošināšanu un personu drošu integrēšanu lomās, kurās tās ietekmē ISMS mērķus.

11.2.2 A pielikuma 6. kontroles pasākums 6.5 – pienākumi pēc darba attiecību izbeigšanas vai darba attiecību nosacījumu maiņas: šī politika pilnībā ievieš kontroles pasākumus atlikušajām piekļuves tiesībām, datu pārvaldībai un līgumiskajiem pienākumiem pēc aiziešanas.

11.2.3 A pielikuma 5.9. kontroles pasākums – personāla pārbaude un 6.2. kontroles pasākums – darba attiecību noteikumi un nosacījumi: darba attiecību uzsākšanas procedūras ietver fona pārbaudi un politikas iepazīšanās apliecināšanas mehānismus atbilstoši šīm prasībām.

11.3 NIST SP 800-53 Rev.5:

11.3.1 PS-4 (Personāla darba attiecību izbeigšana) un PS-5 (Personāla pārcelšana): šī politika nodrošina strukturētu piekļuves tiesību, fizisko piekļuves karšu un aktīvu noņemšanu vai modificēšanu.

11.3.2 AC-2 (Kontu pārvaldība) un AC-6 (Minimālo privilēģiju princips): prasības nodrošina, ka piekļuve ir saskaņota ar lomu un tiek nekavējoties atsaukta, kad tā vairs nav nepieciešama.

11.3.3 IA-4 (Identifikatoru pārvaldība) un IA-5 (Autentifikatoru pārvaldība): atbalsta drošu autentifikācijas datu pārvaldību personāla izmaiņu laikā un pēc tām.

11.3.4 CM-5 (Piekļuves ierobežojumi izmaiņām): novērš nesankcionētas izmaiņas pēc darba attiecību izbeigšanas, atsaucot paaugstinātās piekļuves tiesības.

11.3.5 AU-2 un AU-6: piekļuves notikumu žurnālfiksēšana un izsekojamība tiek stiprināta, izmantojot IAM un audita pierakstu integrāciju.

11.4 EU GDPR (2016/679):

11.4.1 5. panta 1. punkta f) apakšpunkts: aizsargā personas datus pret nesankcionētu piekļuvi, ko šī politika nodrošina, atsaucot lietotāja piekļuvi darbinieka aiziešanas procesa laikā.

11.4.2 32. pants: nosaka pienākumu ieviest atbilstošus tehniskos un organizatoriskos kontroles pasākumus personas datu aizsardzībai nodarbinātības dzīves ciklā.

11.4.3 25. pants – datu aizsardzība pēc projektēšanas un pēc noklusējuma: nodrošina, ka darba attiecību uzsākšanas un izbeigšanas procesos ir integrēta datu minimizēšana, glabāšana un likumīga piekļuves kontrole.

11.4.4 39. apsvērums: uzsver piekļuves ierobežošanu un konfidencialitāti, ko atbalsta šīs politikas struktūra.

11.5 EU NIS2 direktīva (2022/2555):

11.5.1 21. panta 2. punkta b), c), d) apakšpunkts: prasa personāla un operacionālās drošības pasākumus, lai nodrošinātu piekļuves kontroli, iekšējo apdraudējumu mazināšanu un dzīves cikla procesus, kas visi ir atspoguļoti šajā politikā.

11.6 EU DORA (2022/2554):

11.6.1 5. pants – pārvaldība un iekšējā kontrole: šī politika atbalsta iekšējo IKT pārvaldību attiecībā uz cilvēkfaktora risku un piekļuves pārvaldību.

11.6.2 8. pants – IKT risku pārvaldība: piemēro kontroles pasākumus personāla pārejām, kas var pakļaut kritiskos aktīvus vai regulētās vides riskam.

11.6.3 9. pants – incidentu klasifikācija un pārvaldība: nodrošina, ka ar darba attiecību izbeigšanu saistīti pārkāpumi ir ziņojami un mazināmi, izmantojot pareizu piekļuves tiesību atsaukšanu un aktīvu apstrādi.

11.7 COBIT 2019:

11.7.1 APO07 – Pārvaldīti cilvēkresursi: definē lomas, atbildību un dzīves cikla darbības darba attiecību uzsākšanai un izbeigšanai atbilstoši pārvaldības mērķiem.

11.7.2 BAI08 – Zināšanu pārvaldība: stiprina procedūru dokumentēšanu, zināšanu saglabāšanu un kontroles nodošanu darba attiecību beigās.

11.7.3 DSS05 – Pārvaldīti drošības pakalpojumi: nodrošina lietotāju deaktivizāciju, aktīvu kontroli un pārskatatbildību lomu pāreju laikā.

11.7.4 MEA03 – Uzraudzīt, izvērtēt un novērtēt atbilstību: nodrošina, ka darba attiecību uzsākšanas un izbeigšanas kontroles pasākumi tiek izvērtēti iekšējos un ārējos auditos.