					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P04					Dokumenta nosaukums: **Piekļuves kontroles 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	Punkti 5.15, 5.17, 5.18	Loģiskās un fiziskās piekļuves pārvaldība
ISO/IEC 27002:2022	Kontroles pasākumi 8.2, 8.3	Lomās balstīta piekļuve un identitāšu pārvaldība
NIST SP 800-53 Rev. 5	AC-1 līdz AC-20, IA-1 līdz IA-8	Kontu un piekļuves kontroles pasākumi, identitātes autentifikācija
ES GDPR	Panti 5(1)(f), 32(1)(b); apsvērums 39	Datu aizsardzība un minimizēšana
ES NIS2	Pants 21(2)(c–e)	Piekļuves kontrole, lietotāju autentifikācija un aktīvu aizsardzība
ES DORA	Panti 6, 9(2)	IKT lietotāju piekļuve un stingri kontroles pasākumi / trešās puses
COBIT 2019	APO07, BAI03, DSS01, DSS05, MEA03	Personāla piesaiste, operācijas, uzraudzība, atbilstība

1. Mērķis

1.1 Šī politika nosaka obligātos principus, atbildības jomas un kontroles prasības piekļuves pārvaldībai informācijas sistēmām, lietojumprogrammām, fiziskām telpām un datu aktīviem visā organizācijā.

1.2 Tā nodrošina, ka piekļuve tiek piešķirta, pamatojoties uz darba nepieciešamību, amata pienākumiem un riska līmeni, ievērojot minimāli nepieciešamo tiesību principu, principu “jāzina” un pienākumu nošķiršanu.

1.3 Šī politika atbalsta ISO/IEC 27001:2022 5.15. punkta un saistīto kontroles pasākumu ieviešanu, kas reglamentē loģisko un fizisko piekļuvi, lietotāju autentifikāciju un piekļuves dzīves cikla pārvaldību.

1.4 Šī politika nodrošina digitālo un fizisko resursu aizsardzību pret neatļautu izmantošanu, ļaunprātīgu izmantošanu vai kompromitēšanu.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem lietotājiem, sistēmām un objektiem ISMS tvērumā, tostarp:

2.1.1 darbiniekiem, līgumdarbiniekiem, piegādātājiem un pagaidu personālam;

2.1.2 lokālo infrastruktūru, mākoņvidē izvietotām sistēmām un hibrīdvidēm;

2.1.3 visiem korporatīvajiem aktīviem — aparatūrai, programmatūrai, datiem un aizsargātām fiziskām zonām;

2.1.4 loģiskajai piekļuvei (piemēram, sistēmām, tīkliem, lietojumprogrammām, API) un fiziskajai piekļuvei (piemēram, ēkām, datu centriem).

2.2 Tā reglamentē piekļuvi visā identitātes un resursu izmantošanas dzīves ciklā — no personāla pieņemšanas un piekļuves piešķiršanas līdz lomu maiņai un tiesību izbeigšanai.

2.3 Politika attiecas arī uz savu ierīču izmantošanas (BYOD) un attālinātās piekļuves scenārijiem, nodrošinot vienotus kontroles pasākumus neatkarīgi no atrašanās vietas un ierīču īpašumtiesību modeļa.

3. Mērķi

3.1 Ieviest drošus, lomās balstītus piekļuves kontroles pasākumus, kas atbalsta darbības integritāti un atbilstību normatīvajām prasībām.

3.2 Nodrošināt, ka piekļuves tiesības tiek pienācīgi apstiprinātas, uzraudzītas un savlaicīgi atsauktas.

3.3 Novērst neatļautu piekļuvi, privilēģiju eskalāciju un novecojušu piekļuves tiesību saglabāšanos.

3.4 Atbalstīt nulles uzticēšanās principus, pēc noklusējuma liedzot piekļuvi, ja tā nav nepārprotami apstiprināta un pamatota.

3.5 Nodrošināt auditoriem un ieinteresētajām personām pārliecību, izmantojot uz pierādījumiem balstītu, automatizētu piekļuves pārskatīšanu un politikas ieviešanu.

3.6 Integrēt piekļuves kontroli darbības procesos, personāla dzīves cikla notikumos un tehniskajās arhitektūrās.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 Apstiprina piekļuves kontroles politiku un nodrošina atbilstošu budžetu un personāla kapacitāti tās ieviešanai.

4.1.2 Vadības pārskatīšanas ietvaros izvērtē ar piekļuves kontroli saistītos riskus un nosaka atbildību stratēģiskā līmenī.

4.2 CISO / ISMS vadītājs

4.2.1 Atbild par piekļuves kontroles ietvaru un nodrošina tā atbilstību ISO/IEC 27001 un saistītajiem standartiem.

4.2.2 Koordinē politikas ieviešanu, kontroles pasākumu testēšanu un ziņošanu par piekļuves kontroles rādītājiem.

4.2.3 Uzrauga uz risku balstītu piekļuves modelēšanu un seko sistēmiskām kontroles nepilnībām.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Pārskatīšanas ierosinātāji un biežums

9.1.1 Šī politika jāpārskata:

9.1.1.1 reizi gadā; vai

9.1.1.2 pēc būtiskām izmaiņām IT infrastruktūrā, normatīvajās prasībās vai riska situācijā;

9.1.1.3 pēc incidentiem, kas atklāj piekļuves kontroles nepilnības;

9.1.1.4 ja notiek būtiskas izmaiņas autentifikācijas tehnoloģijās vai identitātes platformās.

9.2 Pārskatīšanas pilnvarojums un process

9.2.1 CISO vai norīkots ISMS atbildīgais vada pārskatīšanas ciklu, iekļaujot:

9.2.1.1 iekšējā audita konstatējumus;

9.2.1.2 piekļuves pārskatīšanas rezultātus un rādītājus;

9.2.1.3 juridiskos un regulatīvos atjauninājumus;

9.2.1.4 tehnoloģiju platformu izmaiņas.

9.2.2 Visi grozījumi jāapstiprina izpildvadībai un par tiem jāpaziņo visām ieinteresētajām personām.

9.2.3 Ietekmētajiem lietotājiem pēc būtiskiem atjauninājumiem var tikt prasīts atkārtoti apliecināt iepazīšanos ar politiku.

9.3 Versiju kontrole un dokumentēšana

9.3.1 Pamatversija jāglabā ISMS dokumentu repozitorijā ar šādiem metadatiem:

9.3.1.1 versijas numurs un izmaiņu žurnāls;

9.3.1.2 spēkā stāšanās datums un nākamās pārskatīšanas datums;

9.3.1.3 īpašnieks un apstiprināšanas pilnvarojums;

9.3.1.4 izplatīšanas un apliecinājumu ieraksti.

9.3.2 Aizstātās versijas jāarhivē un jānodrošina to pieejamība vismaz 3 gadus.

10. Saistītās politikas un sasaiste

10.1 Šī politika ir funkcionāli atkarīga no tālāk minētajām politikām un interpretējama kopā ar tām:

10.1.1 P01 – Informācijas drošības politika: nosaka organizācijas drošības saistības un augsta līmeņa piekļuves kontroles prasības.

10.1.2 P03 – Pieļaujamās lietošanas politika: nosaka uzvedības prasības piekļuvei un lietotāju atbildību par atbildīgu sistēmu izmantošanu.

10.1.3 P05 – Izmaiņu pārvaldības politika: nosaka, kā droši jāievieš un jāpārbauda izmaiņas piekļuves konfigurācijās, lomās vai grupu struktūrās.

10.1.4 P07 – Personāla pieņemšanas darbā un darba attiecību izbeigšanas politika: nosaka piekļuves tiesību piešķiršanas uzsākšanu un atsaukšanu atbilstoši lietotāja dzīves cikla notikumiem.

10.1.5 P11 – Lietotāju kontu un privilēģiju pārvaldības politika: nosaka kontu līmeņa kontroles pasākumus un papildina šo politiku ar tehniskām vadlīnijām piekļuves kontroles piemērošanai.

10.2 Kopā šīs politikas nodrošina vienotu un izpildāmu piekļuves pārvaldības ietvaru visās struktūrvienībās un tehnoloģijās.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:2022

11.1.1 Punkts 5.15 – Piekļuves kontrole: šī politika izpilda prasību kontrolēt piekļuvi informācijai un citiem saistītajiem aktīviem, pamatojoties uz darbības un informācijas drošības prasībām.

11.1.2 Punkts 5.17 – Identitātes pārvaldība un punkts 5.18 – Autentifikācijas informācija: šīs prasības tiek īstenotas ar identitāšu piešķiršanu, autentifikācijas mehānismiem un privilēģiju piešķiršanu.

11.1.3 A pielikuma kontroles pasākumi 8.2 (Piekļuves kontroles politika) un 8.3 (Identitātes pārvaldība): nodrošina pamatu šīs politikas kontroles mērķiem, tostarp lomās balstītai piekļuvei, lietotāju dzīves cikla integrācijai un privileģētās piekļuves aizsardzībai.

11.2 NIST SP 800-53 Rev. 5

11.2.1 AC saime (AC-1 līdz AC-20): šī politika atbalsta NIST piekļuves kontroles prasības gan fiziskajām, gan loģiskajām sistēmām, tostarp politikas noteikšanu (AC-1), kontu pārvaldību (AC-2) un pienākumu nošķiršanu (AC-5).

11.2.2 IA saime (IA-1 līdz IA-8): sniedz vadlīnijas identitātes autentifikācijai, autentifikācijas datu aizsardzībai un MFA.

11.2.3 AU-2, AU-12: šīs politikas ietvaros piemērotās žurnalēšanas un auditēšanas prasības atbalsta lietotāju atbildību un incidentu izmeklēšanu.

11.2.4 PE-2 līdz PE-6: aptver fiziskās piekļuves ierobežojumus, kurus šī politika daļēji nodrošina ar caurlaižu kontroli un ēku piekļuves atļaujām.

11.3 ES GDPR (2016/679)

11.3.1 Pants 5(1)(f): personas dati jāaizsargā pret neatļautu piekļuvi. Šī politika nodrošina šī principa tehnisku un procesuālu piemērošanu.

11.3.2 Pants 32(1)(b): prasa ieviest piekļuves kontroles pasākumus, pseidonimizāciju un šifrēšanu, lai novērstu neatļautu personas datu apstrādi.

11.3.3 Apsvērums 39: paredz piekļuves personas datiem minimizēšanu, kas šajā politikā tiek nodrošināta ar minimāli nepieciešamo tiesību principu un prasību pamatot piekļuvi.

11.4 ES NIS2 direktīva (2022/2555)

11.4.1 Pants 21(2)(c–e): šī politika nodrošina tehniskus un organizatoriskus pasākumus piekļuves kontrolei, lietotāju autentifikācijai un aktīvu aizsardzībai būtiskajās un svarīgajās vienībās.

11.5 ES DORA (2022/2554)

11.5.1 Pants 6: prasa IKT riska pārvaldības politikas, kurās skaidri ietverta lietotāju piekļuves pārvaldība un identitātes dzīves cikla kontroles pasākumi. Šī politika izpilda šo prasību finanšu un IKT pakalpojumu sektorā.

11.5.2 Pants 9(2): šī politika atbalsta stingru piekļuves kontroles pasākumu piemērošanu trešo pušu un grupas ietvaros sniegto IKT pakalpojumu pārvaldībā.

11.6 COBIT 2019

11.6.1 APO07 – Pārvaldīti cilvēkresursi: nosaka personāla pieņemšanas darbā un darba attiecību izbeigšanas kontroles pasākumus, lai atbalstītu piekļuves pārvaldību.

11.6.2 BAI03 – Pārvaldīta risinājumu identificēšana un izveide: iekļauj piekļuves kontroles prasības sistēmu izstrādē un izmaiņu procesos.

11.6.3 DSS01 – Pārvaldītas operācijas un DSS05 – Pārvaldīti drošības pakalpojumi: reglamentē loģiskās piekļuves ierobežojumu piemērošanu un pārkāpumu uzraudzību.

11.6.4 MEA03 – Atbilstības uzraudzība, izvērtēšana un novērtēšana: atbalsta audita un pārliecības mehānismus piekļuves kontroles efektivitātes pārbaudei.