					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P04S					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**

Saskaņojums ar standartiem un regulējumiem

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	5. punkts	
ISO/IEC 27002:2022	Kontroles pasākumi 5.15, 5.16, 5.17	
NIST SP 800-53 Rev. 5	AC-1 līdz AC-5	
ES GDPR	32. pants	
ES NIS2	21. panta 2. punkta b) apakšpunkts	
ES DORA	9. pants	
COBIT 2019	APO07, DSS01	

1. Mērķis

1.1. Šī politika nosaka, kā organizācija pārvalda piekļuvi sistēmām, datiem un telpām, lai nodrošinātu, ka informācijai, pamatojoties uz darba nepieciešamību, piekļūst tikai autorizētas personas.

1.2. Tā nosaka skaidrus noteikumus lietotāju piekļuves piešķiršanai, grozīšanai, uzraudzībai un atsaukšanai, lai mazinātu nesankcionētas piekļuves risku un nodrošinātu atbilstību piemērojamajiem tiesību aktiem un standartiem.

1.3. Šī politika ievieš minimālo privilēģiju principu, nosakot, ka piekļuve jāierobežo līdz minimumam, kas nepieciešams darba pienākumu izpildei.

2. Piemērošanas joma

2.1. Šī politika attiecas uz visām personām, kuras izmanto vai pārvalda piekļuvi organizācijas IT sistēmām, tīkliem, datiem vai telpām, tostarp:

2.1.1. darbiniekiem

2.1.2. līgumdarbiniekiem

2.1.3. pagaidu darbiniekiem

2.1.4. ārējiem IT pakalpojumu sniedzējiem

2.2. Tā aptver piekļuvi:

2.2.1. uzņēmuma lietojumprogrammām, failu koplietojumiem un datubāzēm

2.2.2. e-pasta, VPN un attālinātās piekļuves sistēmām

2.2.3. mākoņpakalpojumiem, kas tiek izmantoti uzņēmējdarbības vajadzībām

2.2.4. fiziskajai piekļuvei aizsargājamām telpām, piemēram, birojiem vai serveru telpām

2.3. Šī politika ir saistoša attiecībā uz visām ierīcēm, platformām un atrašanās vietām, tostarp uzņēmuma izsniegtām ierīcēm un apstiprinātām personīgajām ierīcēm BYOD ietvaros.

3. Mērķi

3.1. Nodrošināt, ka piekļuves tiesības tiek piešķirtas tikai pēc formāla apstiprinājuma, pamatojoties uz lomu un darba nepieciešamību.

3.2. Novērst nesankcionētu vai pārmērīgu piekļuvi sensitīviem datiem, sistēmām vai infrastruktūrai.

3.3. Noteikt skaidras procedūras lietotāju piekļuves piešķiršanai, grozīšanai un izbeigšanai.

3.4. Noteikt prasību veikt regulāru piekļuves tiesību pārskatīšanu un nodrošināt automatizētu vai manuālu žurnālfiksēšanu audita vajadzībām.

3.5. Nodrošināt piekļuves ierobežojumu tehnisku izpildi, izmantojot konfigurāciju un uzraudzību.

4. Lomas un atbildība

4.1. Valdes priekšsēdētājs

4.1.1. Apstiprina šo politiku un nodrošina resursu pieejamību efektīvu piekļuves kontroles pasākumu ieviešanai.

4.1.2. Apstiprina izņēmumus un pārskata ikgadējo piekļuves auditu rezultātus.

4.2. IT vadītājs / ārējais IT pakalpojumu sniedzējs

4.2.1. Veic lietotāju kontu piekļuves piešķiršanu, grozīšanu un izbeigšanu.

4.2.2. Uztur piekļuves kontroles reģistru par visām darbībām, tostarp izveidi, izmaiņām un noņemšanu.

4.2.3. Ievieš lomu balstītu piekļuves kontroli un nodrošina spēcīgu autentifikāciju, piemēram, daudzfaktoru autentifikāciju (MFA).

4.2.4. Pārskata piekļuves žurnālus, lai identificētu aizdomīgas darbības, un ziņo par konstatētajām problēmām valdes priekšsēdētājam.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1. Ikgadējā politikas pārskatīšana

9.1.1. IT vadītājam šī politika jāpārskata reizi gadā. Jebkādām izmaiņām tiesiskajā, tehniskajā vai organizatoriskajā kontekstā nekavējoties jāizraisa politikas atjaunināšana.

9.2. Pārskatīšanas ierosinātāji

9.2.1. Politika jāpārskata arī tad, ja notiek kāds no turpmāk minētajiem gadījumiem:

9.2.2. būtiskas sistēmu izmaiņas vai migrācija uz mākoņvidi

9.2.3. izmaiņas lomās vai organizatoriskajā struktūrā

9.2.4. drošības incidents, kas saistīts ar nesankcionētu piekļuvi

9.2.5. regulatīvas izmaiņas, piemēram, GDPR, NIS2 vai DORA atjauninājumi

9.3. Izmaiņu dokumentēšana un izziņošana

9.3.1. Visas pārskatītās redakcijas jāreģistrē, norādot versiju vēsturi un valdes priekšsēdētāja apstiprinājumu, un tās jāpaziņo visam skartajam personālam.

9.4. Pieejamība un apmācība

9.4.1. Šī politika jāpadara pieejama visiem darbiniekiem, un attiecīgā apmācība jānodrošina ievadapmācības procesā un pēc tam reizi gadā.

10. Saistītās politikas un savstarpējā sasaiste

10.1. Šī politika jāpiemēro koordinēti ar turpmāk minētajām SME politikām, lai pilnībā nodrošinātu drošas piekļuves prakses ievērošanu:

10.1.1. P3S – Pieļaujamās izmantošanas politika: nodrošina, ka lietotāji izprot pieļaujamo rīcību piešķirtās piekļuves ietvaros.

10.1.2. P5S – Izmaiņu pārvaldības politika: nodrošina, ka piekļuves tiesības ir saskaņotas ar apstiprinātām sistēmu izmaiņām.

10.1.3. P7S – Darba attiecību uzsākšanas un izbeigšanas politika: nosaka aktivizēšanas punktus lietotāju piekļuves piešķiršanai un atsaukšanai.

10.1.4. P17S – Datu aizsardzības un privātuma politika: nodrošina, ka piekļuves kontroles pasākumi ir saskaņoti ar personas datu aizsardzības prasībām.

10.1.5. P30S – Incidentu reaģēšanas politika: nosaka, kā tiek pārvaldīti un izmeklēti ar piekļuvi saistīti incidenti, piemēram, neatbilstoša izmantošana vai pārkāpumi.

11. Atsauces standarti un ietvari

11.1. ISO/IEC 27001

11.1.1. 5.15. kontroles pasākums nosaka prasību formalizētām piekļuves kontroles politikām un procesiem.

11.2. ISO/IEC 27002

11.2.1. Kontroles pasākumi 5.15–5.17 nosaka detalizētas vadlīnijas lomu balstītai piekļuvei, lietotāju dzīves cikla pārvaldībai un priviliģētas piekļuves pārvaldībai.

11.3. NIST SP 800-53 Rev. 5

11.3.1. AC-1 līdz AC-5 nosaka prasību strukturētām piekļuves pārvaldības politikām, tostarp kontu autorizācijai, pārskatīšanai un uzraudzībai.

11.4. ES GDPR

11.4.1. 32. pants nosaka prasību ieviest tehniskos un organizatoriskos kontroles pasākumus, piemēram, piekļuves pārvaldību, lai nodrošinātu datu drošību un konfidencialitāti.

11.5. ES NIS2 direktīva

11.5.1. 21. panta 2. punkta b) apakšpunkts nosaka prasību operatīvai piekļuves kontrolei un identitātes pārvaldības sistēmām, lai novērstu nesankcionētu piekļuvi sistēmām.

11.6. ES DORA

11.6.1. 9. pants uzsver drošas IKT risku pārvaldības īstenošanu, tostarp stingru piekļuves kontroli finanšu iestādēm.

11.7. COBIT 2019

11.7.1. APO07 – pārvaldīta personāla vadība: nosaka nepieciešamību definēt un ieviest ar piekļuvi saistītās atbildības.

11.7.2. DSS01 – darbību pārvaldība: ietver procedūras loģiskās piekļuves pārvaldībai un drošas operatīvās vides uzturēšanai.