					Šeit ievadiet reģistrētās juridiskās personas nosaukumu						
Dokumenta numurs: P11					Dokumenta nosaukums: **Lietotāju kontu un privilēģiju pārvaldības 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	6.1.3. punkts, 8. punkts	-
ISO/IEC 27002:2022	Kontroles pasākumi 5.15–5.18	-
NIST SP 800-53 Rev.5	AC-1, AC-2, AC-5, AC-6, IA-2–IA-5, AU-2, AU-12	-
ES GDPR	5. panta 1. punkta f) apakšpunkts, 32. pants; 39. apsvērums	-
ES NIS2	21. panta 2. punkta a) un d) apakšpunkts, 21. panta 3. punkts	-
ES DORA	5. pants, 9. pants	-
COBIT 2019	DSS01, DSS05, APO13	-

1. Mērķis

1 Šī politika nosaka obligātos kontroles pasākumus lietotāju kontu un privilēģiju pārvaldībai visās informācijas sistēmās un pakalpojumos. Tā nodrošina, ka piekļuve organizācijas resursiem tiek piešķirta, pamatojoties uz validētu identitāti, amata lomas nepieciešamību, minimāli nepieciešamo tiesību principu un pienākumu nošķiršanas principu.

1.1 Tā atbalsta organizācijas apņemšanos nodrošināt informācijas drošību, ieviešot strukturētus un auditējamus procesus kontu piešķiršanai, privilēģiju piešķiršanai, lietošanas uzraudzībai un kontu atsaukšanai.

1.2 Šī politika ir būtiska, lai mazinātu nesankcionētas piekļuves, privilēģiju neatbilstošas izmantošanas, iekšējo apdraudējumu un neatbilstības piemērojamajiem normatīvajiem un regulatīvajiem ietvariem risku.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visiem darbiniekiem, līgumslēdzējiem, trešo pušu pakalpojumu sniedzējiem, konsultantiem un citām personām, kurām ir piešķirta piekļuve organizācijas IT resursiem, lietojumprogrammām vai datiem.

2.2 Tā attiecas uz visām sistēmām un vidēm, kurās tiek izmantoti lietotāju autentifikācijas un piekļuves kontroles mehānismi, tostarp, bet ne tikai:

2.2.1 Uzņēmuma lietojumprogrammām un datubāzēm

2.2.2 Mākoņplatformām un SaaS vidēm

2.2.3 Operētājsistēmām un administratīvajām konsolēm

2.2.4 Attālās piekļuves rīkiem un VPN

2.2.5 Identitāšu un piekļuves pārvaldības (IAM) sistēmām

2.3 Politika attiecas gan uz standarta, gan priviliģētiem lietotāju kontiem un ietver kontroles pasākumus attiecībā uz:

2.3.1 Kontu izveidi, grozīšanu un deaktivizēšanu

2.3.2 Privilēģiju paaugstināšanu un deleģēšanu

2.3.3 Sesiju kontroli un uzraudzību

2.3.4 Autentifikācijas metodēm un akreditācijas datu pārvaldību

3. Mērķi

3.1 Nodrošināt, ka visi lietotāju konti ir unikāli identificējami, pienācīgi autorizēti un piešķirti tikai pēc formālas nepieciešamības validēšanas.

3.2 Ieviest minimāli nepieciešamo tiesību principu un novērst nevajadzīgu vai pārmērīgu piekļuvi, piemērojot stingrus kontroles pasākumus priviliģētu kontu piešķiršanai un izmantošanai.

3.3 Nodrošināt savlaicīgu kontu statusa atjaunināšanu, pamatojoties uz nodarbinātības vai lomas izmaiņām, tostarp tūlītēju deaktivizēšanu darba attiecību izbeigšanas gadījumā.

3.4 Nodrošināt proaktīvu neaktīvu, neatbilstoši izmantotu vai nesankcionētu kontu identificēšanu un neatbilstību novēršanu, izmantojot žurnalēšanu, pārskatīšanu un automatizāciju.

3.5 Uzturēt atbilstību ISO/IEC 27001:2022 un saistītajiem standartiem, kā arī izpildīt pienākumus saskaņā ar attiecīgajiem normatīvajiem un regulatīvajiem ietvariem, piemēram, GDPR, NIS2, DORA un COBIT 2019.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības speciālists (CISO)

4.1.1 Ir šīs politikas īpašnieks un nodrošina tās ieviešanu visā organizācijā.

4.1.2 Pārskata un apstiprina visus formālos izņēmumus vai ārkārtas piekļuves gadījumus.

4.1.3 Ziņo par ar kontiem saistītajiem audita konstatējumiem un eskalē riskus izpildvadībai.

4.2 Piekļuves kontroles vadītājs / IT administrators

4.2.1 Uztur un darbina tehniskos kontroles pasākumus lietotāju kontu dzīves cikla pārvaldībai.

4.2.2 Veic piekļuves piešķiršanas, piekļuves atsaukšanas un privilēģiju pārvaldības darbības, pamatojoties uz apstiprinātu pieprasījumu.

4.2.3 Uztur autoritatīvu reģistru par visiem lietotāju kontiem, to statusu un privilēģiju līmeni.

4.2.4 Atbalsta auditus un atbilstības pārskatīšanu, nodrošinot žurnālus un darbību pārskatus.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata vismaz reizi gadā vai pēc būtiskām izmaiņām:

9.1.1 Organizācijas struktūrā vai biznesa procesos

9.1.2 IT sistēmās, identitātes platformās vai piekļuves metodēs

9.1.3 Regulatīvajās vai līgumiskajās prasībās, kas saistītas ar identitāšu un piekļuves pārvaldību

9.2 Galvenais informācijas drošības speciālists (CISO) sadarbībā ar piekļuves kontroles vadītāju ir atbildīgs par pārskatīšanas procesa uzsākšanu un iesaistīto pušu atsauksmju koordinēšanu.

9.3 Starpposma pārskatīšanu var ierosināt:

9.3.1 Drošības incidenti, kas saistīti ar kontu nepareizu izmantošanu

9.3.2 Audita konstatējumi, kas norāda uz nepilnībām kontu dzīves cikla pārvaldībā

9.3.3 Jaunu identitāšu vai priviliģētās piekļuves pārvaldības rīku ieviešana

9.4 Šīs politikas atjauninājumiem jābūt:

9.4.1 Pārvaldītiem ar versiju kontroli un reģistrētiem IDPS dokumentācijas bibliotēkā

9.4.2 Paziņotiem visām attiecīgajām iesaistītajām pusēm, tostarp struktūrvienību vadītājiem, IT operācijām un HR

9.4.3 Atbalstītiem ar atjauninātiem apmācību materiāliem un procedūru vadlīnijām

9.5 Visas izmaiņas jāapstiprina izpildvadībai vai informācijas drošības vadības komitejai, un tās jāreģistrē audita vajadzībām.

10. Saistītās politikas un sasaiste

10.1 Šī politika darbības līmenī ir saistīta ar turpmāk minētajām politikām IDPS ietvarā un tiek ar tām atbalstīta:

10.1.1 P4 Piekļuves kontroles politika: nosaka vispārējos piekļuves kontroles principus un mehānismus, tostarp uz noteikumiem balstītus un lomu balstītus kontroles pasākumus.

10.1.2 P7 Darba attiecību uzsākšanas un izbeigšanas politika: nosaka procesuālās darbības lietotāju piekļuves piešķiršanai un izbeigšanai atbilstoši HR procesiem.

10.1.3 P8 Informācijas drošības informētības un apmācību politika: nostiprina lietotāju pienākumus attiecībā uz kontu drošību un autentifikācijas datu aizsardzību.

10.1.4 P13 Datu klasificēšanas un marķēšanas politika: nosaka piekļuves līmeņus atbilstoši datu klasifikācijai, nodrošinot, ka privilēģiju robežas atbilst sensitivitātes līmeņiem.

10.1.5 P22 Žurnālfiksēšanas un uzraudzības politika: nodrošina, ka audita pieraksti tiek vākti par visām ar kontiem saistītajām darbībām un pārskatīti, lai identificētu anomālijas vai nesankcionētu izmantošanu.

10.1.6 P30 Incidentu reaģēšanas politika: regulē eskalāciju, ierobežošanu un pēcincidenta darbības privilēģiju neatbilstošas izmantošanas vai nesankcionētu kontu darbību gadījumos.

10.2 Katra no šīm politikām darbojas kopā, lai visā organizācijā nodrošinātu vienotu, uz risku balstītu identitāšu un piekļuves pārvaldības ietvaru.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiski atzītiem kiberdrošības standartiem un regulatīvajiem ietvariem, kas nosaka drošu identitāšu, piekļuves un privilēģiju pārvaldību kā organizācijas informācijas drošības pamatkomponenti.

11.2 ISO/IEC 27001:

11.2.1 6.1.3. punkts nosaka organizācijām pienākumu noteikt, izvērtēt un apstrādāt informācijas drošības riskus, tādējādi piekļuves un privilēģiju pārvaldību nosakot kā formālu, uz risku balstītu kontroles pasākumu, kas integrēts IDPS plānošanas procesā.

11.2.2 8.1. punkts – darbību plānošana un kontrole: nostiprina tehnisko un procesuālo kontroles pasākumu ieviešanu, kas regulē lietotāju un priviliģēto piekļuvi.

11.3 ISO/IEC 27002:2022 – 5.15. līdz 5.18. kontroles pasākumi:

11.3.1 5.15. kontroles pasākums – lietotāju piekļuves pārvaldība: atbalsta formālus procesus kontu piešķiršanai, piekļuves autorizēšanai un piekļuves tiesību periodiskai pārskatīšanai.

11.3.2 5.16. kontroles pasākums – identitāšu pārvaldība: nosaka identitāšu unikalitāti, dzīves cikla kontroles pasākumus un drošas autentifikācijas piemērošanu.

11.3.3 5.17. kontroles pasākums nodrošina, ka priviliģēto piekļuves tiesību piešķiršana un izmantošana tiek stingri kontrolēta, ir izsekojama un visā lietotāja konta dzīves ciklā atbilst minimāli nepieciešamo tiesību principam.

11.3.4 5.18. kontroles pasākums – Privileged Access Rights: pilnībā īstenots ar lomu balstītu privilēģiju piešķiršanu, auditēšanu un paaugstinātas piekļuves apstiprināšanas prasībām.

11.4 Šie kontroles pasākumi virza strukturētu kontu reģistrēšanas, dereģistrēšanas, privilēģiju nodalīšanas un autentifikācijas informācijas izmantošanas ieviešanu. Politika nodrošina identitāšu dzīves cikla pārvaldību, just-in-time piekļuvi un pastiprinātu sesiju uzraudzību, lai novērstu nesankcionētu sistēmu izmantošanu.

11.5 NIST SP 800-53 Rev.5:

11.5.1 AC-1 (Piekļuves kontroles politika) un AC-2 (Kontu pārvaldība): atspoguļoti politikas prasībās par piekļuves apstiprinājumiem, lomu kartēšanu un lietotāju kontu auditēšanu.

11.5.2 AC-5 (Pienākumu nošķiršana) un AC-6 (Minimāli nepieciešamās tiesības): izpildīti ar privilēģiju ierobežošanu, sasaisti ar amata lomu un divkāršu apstiprinājumu augsta riska uzdevumiem.

11.5.3 IA-2 līdz IA-5 (Identificēšana un autentifikācija): nodrošināti, izmantojot spēcīgus autentifikācijas mehānismus, akreditācijas datu dzīves cikla noteikumus un MFA prasības.

11.5.4 AU-2, AU-12 (Audita žurnālu reģistrēšana un analīze): nodrošināti, izmantojot sesiju ierakstīšanu un priviliģētu darbību uzraudzību sensitīvās vidēs.

11.6 ES GDPR (2016/679):

11.6.1 32. pants – apstrādes drošība: prasa piekļuves kontroles pasākumus un identitātes pārbaudes mehānismus personas datu aizsardzībai. Tas tiek nodrošināts, nosakot pienākumu apstiprināt kontus, pārskatīt privilēģijas un piemērot spēcīgus autentifikācijas aizsardzības pasākumus.

11.6.2 5. panta 1. punkta f) apakšpunkts – integritāte un konfidencialitāte: nodrošina, ka personas datiem piekļūst tikai autorizēti lietotāji ar leģitīmām lomām, ko stiprina šīs politikas prasības kontu pārvaldībai.

11.6.3 39. apsvērums: prasa skaidru piekļuves ierobežošanu un pārskatatbildību — šī politika nodrošina pilnīgu lietotāju identitāšu un privilēģiju piešķīrumu izsekojamību.

11.7 ES NIS2 direktīva (2022/2555):

11.7.1 21. panta 2. punkta a) un d) apakšpunkts: nosaka pienākumu ieviest piekļuves pārvaldības politikas un drošu autentifikācijas datu un priviliģētu sesiju apstrādi, ko atbalsta šīs politikas piešķiršanas, uzraudzības un izņēmumu kontroles pasākumi.

11.7.2 21. panta 3. punkts: veicina piekļuves disciplīnu un augstu identitātes apliecināšanas līmeni kritiskajās nozarēs, ko nodrošina unikālu identifikatoru, RBAC un termiņierobežotas paaugstinātas piekļuves izmantošana.

11.8 ES DORA (2022/2554):

11.8.1 5. pants – IKT pārvaldība un kontrole: nosaka formalizētus procesus IKT lietotāju pārvaldībai, ko aptver dokumentēta piešķiršana, deaktivizēšana un izņēmumu pārvaldība.

11.8.2 9. pants – IKT risku pārvaldība: nosaka organizācijām pienākumu aizsargāt sistēmas, izmantojot piekļuves ierobežojumus un uzraudzību, ko šī politika nodrošina ar MFA, priviliģētas piekļuves žurnalēšanu un centralizētu pārskatīšanu.

11.9 COBIT 2019:

11.9.1 DSS01 – pārvaldītas operācijas: veicina standartizētu darbības kontroles pasākumu ieviešanu, tostarp lietotāju kontu dzīves cikla pārvaldību un piekļuves dokumentēšanu.

11.9.2 DSS05 – pārvaldīti drošības pakalpojumi: atspoguļo drošu lietotāju un sistēmu privilēģiju administrēšanu, atbalstot riska mazināšanu ar minimāli nepieciešamo tiesību principu un audita pierakstu validēšanu.

11.9.3 APO13 – pārvaldīta drošība: nosaka piekļuves pārvaldību digitālajos aktīvos, ko nodrošina formalizēta kontu un lomu autorizācijas prakse ar periodiskas pārskatīšanas prasībām.