					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P11S					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**

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	5.3., 8. punkts	Lomas, pienākumi un darbības plānošana/kontrole lietotāju piekļuves pārvaldībai
ISO/IEC 27002:2022	8. kontrole	Kontroles pasākumi privilēģiju piešķiršanai, pārskatīšanai un atsaukšanai
NIST SP 800-53 Rev.5	AC-2, AC-5, AC-6	Kontu izveide, uzraudzība, minimālo nepieciešamo tiesību piemērošana un pienākumu nošķiršana
ES NIS2	21. panta 2. punkta d) apakšpunkts	Lietotāju piekļuves pārvaldība būtiskām un svarīgām struktūrām
ES DORA	9. panta 2. punkta b) apakšpunkts	Priviliģētas piekļuves kontrole finanšu iestādēs
COBIT 2019	DSS05.03, DSS05.04	Piekļuves tiesību piešķiršana, atņemšana un lietotāju piekļuves periodiska pārskatīšana
ES GDPR	32. pants	Atbilstoši piekļuves kontroles pasākumi personas datu aizsardzībai

1. Mērķis

1.1 Šī politika nosaka prasības lietotāju kontu un piekļuves tiesību pārvaldībai drošā, konsekventā un izsekojamā veidā. Tā nodrošina, ka piekļuve sistēmām un datiem tiek piešķirta tikai autorizētiem lietotājiem un atbilst viņu lomām un pienākumiem.

1.2 Efektīva kontu un privilēģiju pārvaldība ir būtiska, lai novērstu nesankcionētu piekļuvi, mazinātu iekšējos apdraudējumus un nodrošinātu atbilstību ISO/IEC 27001, GDPR un citām normatīvajām prasībām.

1.3 Šī politika ļauj organizācijai noteikt atbildību par kontu izmantošanu, uzraudzīt un auditēt privilēģiju paaugstināšanu, kā arī droši atspējot vai atsaukt piekļuvi, kad tā vairs nav nepieciešama.

1.4 Tā aizsargā organizācijas darbību pret kļūdām vai nepareizu lietošanu, ko izraisa pārmērīga vai neuzraudzīta piekļuve, un palīdz samazināt nejaušas datu noplūdes, privilēģiju ļaunprātīgas izmantošanas vai neatbilstības normatīvajām prasībām risku.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem darbiniekiem, praktikantiem, līgumdarbiniekiem un trešo personu lietotājiem, kuriem ir piekļuve organizācijas IT sistēmām;

2.1.2 visām sistēmām, ierīcēm, pakalpojumiem un platformām, ko pārvalda organizācija vai kas tiek pārvaldītas tās vārdā, tostarp mākoņpakalpojumiem, lokālajai infrastruktūrai un trešo personu rīkiem.

2.2 Tā aptver visu veidu lietotāju kontus, tostarp:

2.2.1 vārdiskos lietotāju kontus (piemēram, e-pasta kontus, sistēmu pieteikšanās kontus);

2.2.2 administratoru un sistēmas līmeņa kontus;

2.2.3 pagaidu, viesu vai trešo personu piekļuves autentifikācijas datus;

2.2.4 servisa kontus, ko izmanto lietotnes vai automatizācijas sistēmas.

2.3 Politika ir piemērojama visā konta dzīves ciklā — no izveides un apstiprināšanas līdz izmaiņām, uzraudzībai un deaktivizēšanai. Tas ietver sākotnējo piekļuves piešķiršanu darbā pieņemšanas procesā, piekļuves tiesību pārskatīšanu lomu maiņas laikā un piekļuves tiesību atsaukšanu darba attiecību izbeigšanas laikā.

3. Mērķi

3.1 Piešķirt visiem sistēmu lietotājiem unikālas un izsekojamas lietotāju identitātes, nodrošinot pārskatatbildību un novēršot koplietotu autentifikācijas datu izmantošanu.

3.2 Piemērot minimālo nepieciešamo tiesību principu, nodrošinot, ka lietotājiem tiek piešķirts tikai darba pienākumu izpildei nepieciešamais minimālais piekļuves līmenis.

3.3 Novērst nesankcionētu piekļuvi sensitīvām sistēmām vai datiem, izmantojot skaidri dokumentētus apstiprināšanas un pārskatīšanas procesus.

3.4 Nodrošināt savlaicīgu lietotāju kontu deaktivizēšanu, ja tie vairs nav nepieciešami, piemēram, izbeidzot darba attiecības, beidzoties līgumam vai mainoties lomai.

3.5 Uzturēt drošu un auditam gatavu vidi, dokumentējot visas kontu izmaiņas, apstiprinājumus un periodiskās pārskatīšanas.

3.6 Nodrošināt, ka privilēģiju paaugstināšana tiek stingri kontrolēta, neatkarīgi apstiprināta un reģistrēta žurnālos, un ka paaugstinātā piekļuve tiek nekavējoties atsaukta, tiklīdz tā vairs nav nepieciešama.

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 Ir vispārēji atbildīgs par šīs politikas ievērošanas nodrošināšanu.

4.1.2 Nodrošina, ka kontu pārvaldības prakse atbilst ISO/IEC 27001 sertifikācijas prasībām un piemērojamajām tiesību aktu prasībām (piemēram, GDPR).

4.1.3 Par jebkuru nesankcionētu piekļuvi, drošības incidentu vai ar lietotāju kontiem saistītu politikas pārkāpumu viņš ir nekavējoties jāinformē.

4.1.4 Pārrauga politikas pārskatīšanu, auditus un politikas izpildes pasākumus.

4.2 IT vadītājs vai ārējais IT pakalpojumu sniedzējs

4.2.1 Atbild par kontu un privilēģiju kontroles pasākumu tehnisko ieviešanu visās organizācijā izmantotajās sistēmās.

4.2.2 Drīkst veikt lietotāju kontu piekļuves piešķiršanu, izmaiņas un deaktivizēšanu tikai, pamatojoties uz dokumentētu apstiprinājumu.

4.2.3 Nodrošina paroļu sarežģītības prasību, ekrāna automātiskās bloķēšanas, daudzfaktoru autentifikācijas (MFA) (ja tā ir pieejama) un sistēmu žurnālfiksēšanas piemērošanu.

4.2.4 Uztur drošus ierakstus par visiem piekļuves apstiprinājumiem, kontu īpašumtiesībām, privilēģiju paaugstināšanu un piekļuves tiesību atsaukšanu.

4.2.5 Veic nesankcionētu vai bāreņkontu uzraudzību un ziņo ģenerāldirektoram par neatbilstībām.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika ģenerāldirektoram un IT vadītājam jāpārskata vismaz reizi gadā, lai nodrošinātu atbilstību:

9.1.1 spēkā esošajiem ISO/IEC 27001:2022 kontroles pasākumiem un vadlīnijām;

9.1.2 normatīvo prasību atjauninājumiem (piemēram, GDPR, DORA, NIS2);

9.1.3 izmaiņām sistēmās, pakalpojumos vai organizācijas struktūrā.

9.2 Pārskatīšana jāveic arī pēc:

9.2.1 būtiskiem drošības incidentiem vai audita konstatējumiem;

9.2.2 nozīmīgām izmaiņām IT sistēmās vai kontu arhitektūrā;

9.2.3 jaunu platformu ieviešanas, kurām nepieciešama piekļuves kontroles integrācija.

9.3 Visas izmaiņas jāapstiprina ģenerāldirektoram un skaidri jāpaziņo ietekmētajiem darbiniekiem.

10. Saistītās politikas un sasaiste

10.1 P2S – Pārvaldības lomu un atbildības politika: nosaka pārskatatbildību un lēmumu pieņemšanas pilnvaras piekļuves apstiprināšanai un pārraudzībai.

10.2 P4S – Piekļuves kontroles politika: nosaka sistēmu līmeņa piekļuves kontroles piemērošanu un autentifikācijas metodes.

10.3 P7S – Darba attiecību uzsākšanas un izbeigšanas politika: nodrošina, ka kontu izveide un noņemšana ir iekļauta personāla izmaiņu procesos, ko pārvalda personāla funkcija.

10.4 P8S – Informācijas drošības informētības un apmācību politika: nodrošina lietotāju apmācību par drošu kontu izmantošanas praksi un lietošanas prasībām.

10.5 P30S – Incidentu reaģēšanas politika: nosaka darbības, kas jāveic, ja konta nepareiza lietošana izraisa drošības incidentu vai nesankcionētu izpaušanu.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 5.3. punkts: nosaka, ka informācijas drošības lomas un pienākumi ir skaidri jāpiešķir un jānodrošina to ievērošana.

11.1.2 8.1. punkts: darbības plānošanā un kontrolē jāietver lietotāju piekļuves pārvaldība.

11.2 ISO/IEC 27002

11.2.1 8.2. kontrole: nosaka tehniskos un procesu kontroles pasākumus paaugstinātu privilēģiju piešķiršanai, pārskatīšanai un atsaukšanai.

11.3 NIST SP 800-53 Rev.5

11.3.1 AC-2: nosaka kontu izveidi, uzraudzību un atsaukšanu atbilstoši noteiktām lomām un procesiem.

11.3.2 AC-5: nosaka pienākumu nošķiršanu, lai novērstu interešu konfliktus vai privilēģiju ļaunprātīgu izmantošanu.

11.3.3 AC-6: nosaka minimālo nepieciešamo tiesību principa piemērošanu visām piekļuves tiesībām.

11.4 ES GDPR

11.4.1 32. pants: nosaka atbilstošus piekļuves kontroles pasākumus personas datu aizsardzībai pret nesankcionētu piekļuvi vai izmaiņām.

11.5 ES NIS

11.5.1 21. panta 2. punkta d) apakšpunkts: nosaka lietotāju piekļuves pārvaldību kā daļu no būtiskiem drošības kontroles pasākumiem būtiskām un svarīgām struktūrām.

11.6 ES DORA

11.6.1 9. panta 2. punkta b) apakšpunkts: nosaka, ka finanšu iestādēm jāievieš piekļuves kontroles pasākumi, kas ierobežo un uzrauga privileģētās tiesības.

11.7 COBIT 2019

11.7.1 DSS05.03: nosaka piekļuves tiesību piešķiršanu un atņemšanu kā daļu no IT pārvaldības.

11.7.2 DSS05.04: paredz nepārtrauktu lietotāju piekļuves pārskatīšanu un saskaņošanu ar organizācijas lomām.