					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P02S					Dokumenta nosaukums: **Pārvaldības lomu un atbildības 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 regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	5. punkts	
ISO/IEC 27002:2022	Kontroles pasākumi: 5.2, 5.3, 5	
NIST SP 800-53 Rev.5	PM-1, PL-1, PL-4, CA-1, AC-1	
ES VDAR	5. panta 2. punkts, 32. pants	

1. Mērķis

1.1 Šī politika nosaka, kā organizācijā tiek piešķirtas, deleģētas un pārvaldītas informācijas drošības pārvaldības atbildības, lai nodrošinātu pilnīgu atbilstību ISO/IEC 27001:2022 un citām normatīvajām prasībām.

1.2 Tā nodrošina skaidru atbildību noteikšanu visos līmeņos un veicina darbības efektivitāti, skaidri nosakot, kura persona ir atbildīga par katru ar drošību saistīto funkciju.

1.3 Šī politika stiprina gatavību auditam un veicina klientu uzticēšanos, apliecinot formālu drošības pārvaldību arī organizācijās ar ierobežotiem tehniskajiem resursiem vai ārpakalpojumā sniegtiem IT pakalpojumiem.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām personām, kuras strādā ar organizācijas sistēmām vai datiem, tostarp:

2.1.1 Uzņēmuma īpašniekiem un ģenerāldirektoriem

2.1.2 Darbiniekiem un līgumdarbiniekiem

2.1.3 Ārējiem IT pakalpojumu sniedzējiem vai konsultantiem

2.2 Tā aptver visas sistēmas, vides un pakalpojumus, ko izmanto uzņēmuma vai klientu informācijas apstrādei, pārsūtīšanai vai glabāšanai, tostarp:

2.2.1 Biroja IT infrastruktūru un attālinātā darba ierīces

2.2.2 Mākoņplatformas un e-pasta pakalpojumus

2.2.3 Fiziskos ierakstus un koplietojamos diskus

2.3 Piemērošanas joma ietver gan iekšējās darbības, gan ārpakalpojumā nodotas darbības, kas saistītas ar informācijas drošības pārvaldību.

3. Mērķi

3.1 Noteikt skaidru atbildību par visiem ar drošību saistītajiem pienākumiem, tostarp politiku pārvaldību, piekļuves kontroli, incidentu apstrādi un uzraudzību.

3.2 Nodrošināt efektīvu pienākumu nošķiršanu, lai mazinātu interešu konfliktu vai krāpšanas risku.

3.3 Nodrošināt, ka drošības uzdevumi un lomas ir skaidri dokumentēti un regulāri pārskatīti.

3.4 Nodrošināt informētu lēmumu pieņemšanu, eskalāciju un IT un drošības risku pārraudzību.

3.5 Atbalstīt ISO/IEC 27001:2022 sertifikāciju un stiprināt klientu, partneru un auditoru uzticību.

4. Lomas un atbildība

4.1 Ģenerāldirektors / uzņēmuma īpašnieks

4.1.1 Ir pilnībā atbildīgs par šīs politikas ieviešanu un uzraudzību.

4.1.2 Apstiprina visas drošības lomas, atbildības un deleģēšanas lēmumus.

4.1.3 Uzrauga atbilstību un pieņem galīgos lēmumus par politikas izņēmumiem un eskalāciju.

4.2 Norīkots drošības koordinators (ja iecelts)

4.2.1 Šo lomu var pildīt darbinieks vai uzticams konsultants.

4.2.2 Mikrouzņēmuma vidē šo lomu var uzņemties ģenerāldirektors vai ārējs pakalpojumu sniedzējs.

4.2.3 Sniedz atbalstu ikdienas piekļuves kontroles nodrošināšanā, reaģēšanā uz incidentiem un pamata tehnisko drošības uzdevumu izpildē.

4.2.4 Tieši ziņo ģenerāldirektoram par jebkādiem drošības jautājumiem vai riskiem.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ikgadējā pārskatīšana

9.1.1 Ģenerāldirektoram šī politika jāpārskata ik pēc 12 mēnešiem, lai nodrošinātu, ka tā joprojām atspoguļo juridiskās prasības, darbības vajadzības un ISO/IEC 27001 sertifikācijas prasības.

9.2 Starpposma pārskatīšana

9.2.1 Pārskatīšana jāveic arī tad, ja:

9.2.1.1 Notiek būtiskas organizatoriskas izmaiņas

9.2.1.2 Tiek piesaistīts jauns pakalpojumu sniedzējs

9.2.1.3 Notiek nopietns drošības incidents

9.2.1.4 Tiek atjaunināts VDAR, NIS2 vai DORA regulējums

9.3 Versiju kontrole un dokumentēšana

9.3.1 Katrā pārskatīšanā jāiekļauj:

9.3.1.1 Pārskatīšanas datums

9.3.1.2 Jebkādu izmaiņu kopsavilkums

9.3.1.3 Ģenerāldirektora paraksts vai dokumentēts apstiprinājums

9.3.1.4 Arhivētas iepriekšējās versijas atsaucei auditā

9.4 Izmaiņu paziņošana

9.4.1 Visi politikas atjauninājumi nekavējoties jāpaziņo darbiniekiem un pakalpojumu sniedzējiem pa e-pastu, iekšējos portālos vai ar formāliem paziņojumiem.

10. Saistītās politikas un sasaistes

10.1 Šī politika pilnīgai efektivitātei jāievieš kopā ar šādām SME politikām:

10.1.1 P4S – Piekļuves kontroles politika: nosaka, kā piekļuve tiek piešķirta, pārvaldīta un atsaukta, tieši sasaistot to ar piešķirtajām lomām un uzraudzību.

10.1.2 P8S – Informācijas drošības informētības un apmācību politika: nostiprina lomām specifiskos pienākumus un gaidas.

10.1.3 P17S – Datu aizsardzības un privātuma politika: nosaka juridiskos pienākumus saskaņā ar VDAR, kas tiek piešķirti šajā pārvaldības politikā noteiktajām lomām.

10.1.4 P30S – Reaģēšanas uz incidentiem politika: nosaka konkrētas atbildības par incidentu ziņošanu, eskalāciju un novēršanu.

10.2 Kopā šīs politikas nodrošina konsekventu piemērošanu, iekšējo atbildību un ārējo atbilstību.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 5.3. punkts – Organizatoriskās lomas, atbildība un pilnvaras: nosaka, ka lomas ir skaidri jāpiešķir un augstākajai vadībai tās jāatbalsta.

11.2 ISO/IEC 27002

11.2.1 Kontroles pasākumi 5.2–5.4: nosaka pienākumu skaidri dokumentēt informācijas drošības lomas, nodrošināt pienākumu nošķiršanu un vadības uzraudzību.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1: nosaka visaptverošu informācijas drošības programmu ar noteiktām atbildībām.

11.3.2 PL-1 līdz PL-4: paredz plānošanas kontroles pasākumus, tostarp politiku izstrādi un dokumentētu lomu piešķiršanu.

11.3.3 CA-1: nosaka izvērtēšanas un autorizācijas lomu definēšanu.

11.3.4 AC-1: sasaista uz lomām balstītu piekļuves kontroli ar piešķirtajām pārvaldības atbildībām.

11.4 ES VDAR

11.4.1 5. panta 2. punkts – Pārskatatbildība: nosaka organizācijām pienākumu pierādīt atbilstību attiecībā uz lomām un atbildībām.

11.4.2 32. pants – Apstrādes drošība: uzsver skaidru pienākumu piešķiršanu personas datu aizsardzībai.

11.5 ES NIS

11.5.1 21. panta 2. punkta a) apakšpunkts: nosaka pārvaldības struktūras, kurās ietvertas formalizētas lomas kiberrisku un incidentu pārvaldībai.

11.6 ES DORA

11.6.1 9. un 10. pants: prasa finanšu iestādēm skaidri piešķirt un uzraudzīt ar IKT un drošību saistītās atbildības.

11.7 COBIT 2019

11.7.1 EDM03 – Nodrošināt riska optimizāciju: prasa skaidri noteiktas lomas un eskalācijas ceļus drošības risku pārvaldībai.

11.7.2 APO13 – Pārvaldīt drošību: piešķir stratēģiskos un operatīvos drošības pienākumus personām un lomām.

11.7.3 DSS05 – Pārvaldīt drošības pakalpojumus: nosaka nepieciešamību pēc struktūras un izsekojamības atbildībām par ārējiem un iekšējiem drošības pakalpojumiem.