					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P06S					Dokumenta nosaukums: **Risku 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

Saskaņojums ar standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1., 6.1. punkts	
ISO/IEC 27002:2022	5.4, 5.25	
NIST SP 800-53 Rev.5	RA-1 līdz RA-7, PM-9	
ES NIS2	21. panta 2. punkta a–d apakšpunkts	
ES DORA	5. pants	
COBIT 2019	APO12, MEA	

1. Mērķis

1.1 Šī politika nosaka, kā organizācija identificē, novērtē un pārvalda riskus, kas saistīti ar informācijas drošību, darbību, tehnoloģijām un trešo pušu pakalpojumiem.

1.2 Tā nodrošina, ka risku pārvaldība ir neatņemama plānošanas, projektu īstenošanas, piegādātāju atlases un incidentu apstrādes sastāvdaļa atbilstoši ISO 27001, ISO 31000 un normatīvo aktu prasībām.

1.3 Politika atbalsta informētu lēmumu pieņemšanu, informācijas aktīvu aizsardzību un būtisko darbības procesu noturību.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visām organizācijas struktūrvienībām, sistēmām un lietotājiem;

2.1.2 visu informāciju, pakalpojumiem un aktīviem, ko pārvalda iekšēji vai ar trešo pušu starpniecību;

2.1.3 ar riskiem saistītām darbībām, tostarp projektu pārskatīšanu, sistēmu atjaunināšanu, ārpakalpojumiem un normatīvās atbilstības nodrošināšanu.

2.2 Tā aptver visu veidu riskus, tostarp:

2.2.1 kiberdrošības apdraudējumus un sistēmu ievainojamības;

2.2.2 darbības traucējumus un pakalpojumu nepieejamību;

2.2.3 tiesiskos, atbilstības un reputācijas riskus;

2.2.4 trešo pušu un piegādes ķēdes riskus.

2.3 Visiem darbiniekiem, līgumdarbiniekiem un pakalpojumu sniedzējiem, identificējot vai ziņojot par riskiem, ir jāievēro šī politika.

3. Mērķi

3.1 Integrēt vienkāršas un atkārtojamas riska novērtēšanas procedūras ikdienas darbības procesos.

3.2 Identificēt un prioritizēt riskus, kas var ietekmēt konfidencialitāti, integritāti un pieejamību (CIA) vai tiesisko atbilstību.

3.3 Noteikt risku īpašumtiesības un definēt riska apstrādes darbības visiem būtiskajiem riskiem.

3.4 Uzturēt precīzu un aktuālu risku reģistru, lai nodrošinātu gatavību auditam un risku izsekojamību.

3.5 Nodrošināt vadības iesaisti riska tolerances un būtisku risku apstrādes plānu apstiprināšanā.

4. Lomas un atbildība

4.1 Vispārējais vadītājs

4.1.1 Nosaka organizācijas riska apetīti un apstiprina risku pārvaldības ietvaru.

4.1.2 Apstiprina būtiskus lēmumus par risku apstrādi un nepieciešamo resursu piešķiršanu.

4.1.3 Reizi ceturksnī kopā ar risku koordinatoru pārskata būtiskākos riskus.

4.2 Risku koordinators (vai ISMS īpašnieks)

4.2.1 Organizē riska novērtēšanas veikšanu un uztur risku reģistru.

4.2.2 Nodrošina, ka riska novērtējums, risku īpašumtiesības un riska apstrādes darbības tiek dokumentētas.

4.2.3 Organizē vismaz vienu formālu risku pārskatīšanu gadā.

[... 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 Šī politika jāpārskata vismaz reizi gadā vispārējam vadītājam un risku koordinatoram, lai nodrošinātu tās atbilstību un pilnīgumu.

9.2 Atjaunināšanas ierosinātāji

9.2.1 Agrāka pārskatīšana un atjaunināšana jāveic, ja:

9.2.1.1 būtisks incidents vai audita konstatējums atklāj kontroles nepilnības risku pārvaldībā;

9.2.1.2 tiek ieviestas jaunas biznesa vienības, tehnoloģijas vai partnerības;

9.2.1.3 mainās normatīvās vai līgumiskās prasības.

9.3 Versiju kontrole

9.3.1 Visi šīs politikas atjauninājumi jāversē ar šādiem metadatiem:

9.3.1.1 versijas numurs un spēkā stāšanās datums;

9.3.1.2 izmaiņu kopsavilkums;

9.3.1.3 apstiprinātājs (vispārējais vadītājs);

9.3.1.4 arhivētās iepriekšējās versijas audita vajadzībām.

9.4 Komunikācija un informētība

9.4.1 Politikas atjauninātās versijas un būtiskie risku apstrādes plāni jāpaziņo ietekmētajiem darbiniekiem. Ikgadējā informētības apmācībā jāiekļauj risku izpratnes pamatprincipi.

10. Saistītās politikas un sasaistes

10.1 Šī politika tiek īstenota koordinēti ar citām politikām, lai nodrošinātu visaptverošu drošības pārvaldību:

10.1.1 P2S – Pārvaldības lomu un atbildības politika: nosaka, kurš ir atbildīgs par risku īpašumtiesībām un lēmumu pieņemšanu.

10.1.2 P5S – Izmaiņu pārvaldības politika: nosaka riska novērtēšanas veikšanu pirms tehnisku vai procesu izmaiņu ieviešanas.

10.1.3 P17S – Datu aizsardzības un privātuma politika: aptver regulatīvos riskus, kas saistīti ar personas datu apstrādi.

10.1.4 P30S – Incidentu reaģēšanas politika: nodrošina, ka riska apstrāde turpinās drošības incidentu laikā un pēc tiem.

10.1.5 P33S – Darbības nepārtrauktības politika: identificē atlikušo risku un atjaunošanas pasākumus kritiskajiem pakalpojumiem.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:

11.1.1 6.1. punkts – nosaka formālu risku pārvaldības procesu un riska apstrādes plānošanu.

11.1.2 6.1.3. punkts – nosaka prasību organizācijām uzturēt dokumentētus riska apstrādes plānus un apstiprinājumus.

11.2 ISO/IEC 27002:

11.2.1 5.4. un 5.25. kontrole – sniedz ieviešanas vadlīnijas par risku īpašumtiesībām, prioritizēšanu un dzīves cikla pārvaldību.

11.3 NIST SP 800-53 Rev.:

11.3.1 RA-1 līdz RA-7 – definē riska novērtēšanu, reaģēšanas stratēģijas, dokumentēšanu un pārskatīšanas mehānismus.

11.4 PM-9 – nosaka konsekventu organizācijas risku uzraudzību vadības līmenī.

11.5 ES NIS2 direktīva

11.5.1 21. panta 2. punkta a–d apakšpunkts – uzliek būtiskajiem un svarīgajiem subjektiem pienākumu īstenot riska novērtēšanas, riska mazināšanas un pārvaldības kontroles pasākumus.

11.6 ES DORA

11.6.1 5. pants – nosaka regulētajām vienībām pienākumu definēt un pārvaldīt IKT riska pārvaldības ietvaru, tostarp identificēšanu, klasificēšanu un reaģēšanu.

11.7 COBIT 2019

11.7.1 APO12 – Risku pārvaldība: integrē riskus stratēģiskajā un operatīvajā plānošanā.

11.7.2 MEA01 – Uzraudzīt, izvērtēt un novērtēt: nodrošina risku procesu un darbību efektivitāti un atbilstību.