					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P02					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**

Saskaņota ar standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkts 5.3; A pielikuma kontroles pasākums 5	
ISO/IEC 27002:2022	Kontroles pasākums 5	
NIST SP 800-53 Rev.5	PL-1 līdz PL-4, PM-1 līdz PM-13	
ES GDPR	Panti 5(1)(f), 24, 37	
ES NIS2	Pants 21(2)(a)	
ES DORA	Pants 5	
COBIT 2019	EDM01, EDM02, APO01, APO12, MEA	

1. Mērķis

1.1 Šī politika nosaka pārvaldības modeli, organizatoriskās lomas un atbildību, kas nepieciešama efektīvai informācijas drošības pārvaldības sistēmas (ISMS) darbībai.

1.2 Tā nosaka skaidras atbildības robežas, lēmumu pieņemšanas pilnvaras un eskalācijas ceļus, lai nodrošinātu, ka informācijas drošība ir integrēta visos organizācijas līmeņos un saskaņota ar stratēģiskajiem darbības mērķiem.

1.3 Šī politika īsteno ISO/IEC 27001:2022 5. punkta un A.5.2 kontroles pasākuma prasības, nodrošinot, ka ar drošību saistīto darbību atbildība ir skaidri noteikta, dokumentēta, izziņota un periodiski pārskatīta.

1.4 Šī politika nodrošina arī pamatu integrētai pārvaldībai ar citām jomām, piemēram, risku pārvaldību, atbilstību, IT darbību un juridisko funkciju.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām personām un vienībām, kas iesaistītas informācijas drošības pārvaldībā, nodrošināšanā un uzraudzībā ISMS tvērumā. Tas ietver:

2.1.1 izpildvadību, augstāko vadību un valdes locekļus;

2.1.2 ISMS vadītājus, CISO un kontroles pasākumu īpašniekus;

2.1.3 procesu un aktīvu īpašniekus;

2.1.4 līgumdarbiniekus un trešo pušu pakalpojumu sniedzējus, kuriem deleģēta atbildība drošības jomā.

2.2 Tā aptver gan iekšējās funkcijas, gan ārpakalpojumā nodrošinātas funkcijas (piemēram, ārpakalpojumā sniegtu SOC vai mākoņplatformu administratorus), ja pārvaldības lomas ir formāli piešķirtas vai noteiktas līgumiski.

2.3 Šī politika attiecas arī uz organizācijas struktūrvienībām, nodaļām un projektu komandām, kas pārvalda vai ietekmē drošībai nozīmīgus aktīvus, sistēmas vai pakalpojumus.

3. Mērķi

3.1 Nodrošināt, ka informācijas drošības lomas un atbildība ir formāli noteikta, piešķirta, izziņota un dokumentēta.

3.2 Uzturēt pārvaldības modeli, kas nodrošina pienākumu nošķiršanu, novērš interešu konfliktus un ļauj eskalēt neatrisinātus drošības jautājumus.

3.3 Nodrošināt, ka atbildība un pilnvaras drošības lēmumu pieņemšanai tiek sadalītas atbilstoši ietekmei uz darbību un organizācijas struktūrai.

3.4 Izveidot ietvaru deleģējumu pārvaldībai, lomu izmaiņām un piešķirtās atbildības pārskatīšanai.

3.5 Sniegt ieinteresētajām pusēm, tostarp regulatoriem, auditoriem un klientiem, pārliecību, ka informācijas drošība tiek pārvaldīta efektīvi un atbilstoši piemērojamiem standartiem.

4. Lomas un atbildība

4.1 Izpildvadība (augstākā vadība)

4.1.1 Nodrošina stratēģisko uzraudzību, piešķir resursus un nodrošina saskaņotību starp ISMS mērķiem un organizācijas darbības mērķiem.

4.1.2 Apstiprina galveno ISMS dokumentāciju, tostarp informācijas drošības politiku, riska apstrādes plānus un lēmumus par audita neatbilstību novēršanu.

4.1.3 Piedalās ISMS vadības pārskatē un eskalē lēmumus, kuriem nepieciešams valdes līmeņa apstiprinājums.

4.1.4 Veicina drošības kultūru un sekmē organizācijas atbilstību drošības pārvaldības principiem.

4.2 Informācijas drošības vadības komiteja (ISSC)

4.2.1 Darbojas kā starpfunkcionāla pārvaldības institūcija ISMS uzraudzībai.

4.2.2 Pārskata riska stāvokli, kontroles pasākumu efektivitāti, audita konstatējumus un stratēģiskās drošības iniciatīvas.

4.2.3 Veicina koordināciju starp struktūrvienībām (piemēram, IT, juridisko funkciju, personālvadību, risku pārvaldību, atbilstību un darbības nodrošināšanu).

4.2.4 Apstiprina eskalācijas sliekšņus, budžeta sadalījumu un politiku izmaiņas, kurām nepieciešama izpildvadības iesaiste.

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

9. Pārskatīšanas un aktualizēšanas prasības

9.1 Pārskatīšanas grafiks

9.1.1 Šī politika jāpārskata vismaz reizi gadā vai, ja notiek:

9.1.1.1 izmaiņas organizācijas struktūrā vai izpildvadības sastāvā;

9.1.1.2 ISMS tvēruma paplašināšana vai pārdefinēšana;

9.1.1.3 regulatīvas izmaiņas, kas ietekmē lomu piešķīrumu vai uzraudzību;

9.1.1.4 būtiski audita konstatējumi vai incidenti, kas saistīti ar pārvaldības kļūmēm.

9.2 Pārskatīšanas un apstiprināšanas process

9.2.1 ISMS vadītājs ierosina un vada pārskatīšanas procesu, tostarp ieinteresēto pušu ieguldījuma un audita atgriezeniskās saites apkopošanu.

9.2.2 Ierosinātie atjauninājumi jāpārskata ISSC un formāli jāapstiprina izpildvadībai.

9.2.3 Katra versija jāuzskaita ISMS dokumentu reģistrā un tajā jāiekļauj šāda metainformācija:

9.2.3.1 politikas identifikators un nosaukums;

9.2.3.2 versijas numurs un izmaiņu kopsavilkums;

9.2.3.3 spēkā stāšanās datums un nākamās pārskatīšanas datums;

9.2.3.4 politikas īpašnieks un apstiprinātājs;

9.2.3.5 dokumenta klasifikācijas līmenis;

9.2.3.6 glabāšanas un arhivēšanas vēsture.

10. Saistītās politikas un sasaistes

10.1 Šī politika interpretējama kopā ar šādām politikām:

10.1.1 P1 – Informācijas drošības politika: nosaka kopējo drošības programmu un iezīmē vadības atbildību par politikas apstiprināšanu un stratēģisko uzraudzību.

10.1.2 P5 – Izmaiņu pārvaldības politika: nodrošina, ka izmaiņas pārvaldības struktūrās, lomās vai atbildībā tiek pakļautas dokumentētam apstiprinājumam un risku pārskatīšanai.

10.1.3 P6 – Risku pārvaldības politika: identificē un apstrādā pārvaldības riskus, kas izriet no lomu konfliktiem, nepiešķirtiem pienākumiem vai eskalācijas trūkuma.

10.1.4 P7 – Personāla uzņemšanas un darba attiecību izbeigšanas politika: nodrošina kontroles pasākumu piešķiršanas un atsaukšanas procesus personāla dzīves cikla izmaiņu laikā.

10.1.5 P33 – Audita un atbilstības uzraudzības politika: atbalsta neatkarīgu pārvaldības efektivitātes pārskatīšanu un nosaka korektīvās darbības neatbilstības gadījumā.

10.2 Šīs politikas kopumā atbalsta vienotu un piemērojamu ISMS pārvaldības ietvaru.

11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiski atzītiem informācijas drošības pārvaldības un lomu atbildības standartiem un ietvariem. Tā nodrošina izsekojamību līdz regulatīvajām un sertifikācijas prasībām un atbalsta pamatotu ISMS struktūru.

11.2 ISO/IEC 27001

11.2.1 Punkts 5.3 – Organizatoriskās lomas, atbildība un pilnvaras: šī politika izpilda prasību, ka ar informācijas drošību saistītajām lomām jābūt skaidri piešķirtām, izziņotām un dokumentētām.

11.2.2 Punkts 9.3 – Vadības pārskate: šī politika nodrošina izpildvadības uzraudzību pār ISMS lomām un pārvaldību, izmantojot ceturkšņa un ikgadējo pārskatīšanu.

11.2.3 A pielikuma kontroles pasākums 5.2 – Informācijas drošības lomas un atbildība: nosaka lomas tehniskajā, operacionālajā un stratēģiskajā līmenī, lai nodrošinātu pienākumu nošķiršanu, riska īpašumtiesības un izsekojamu atbildību.

11.3 ISO/IEC 27002:2022 – Kontroles pasākums 5

11.3.1 Tas sniedz ieviešanas vadlīnijas informācijas drošības atbildības piešķiršanai visā organizācijā. Šī politika ievēro minētās vadlīnijas, nosakot lomu tipus, deleģēšanas noteikumus, eskalācijas procedūras un pārskatīšanas mehānismus.

11.4 NIST SP 800-53 Rev.5

11.4.1 PL-1 līdz PL-4: nosaka nepieciešamību pēc formālas plānošanas dokumentācijas, tostarp politikām, kas definē pārvaldību un piešķir drošības atbildību.

11.4.2 PM-1 (Informācijas drošības programmas plāns) un PM-2 (Vecākais informācijas drošības vadītājs): šajā politikā tas atspoguļots ar CISO/ISMS vadītāja un formālu pārvaldības lomu noteikšanu.

11.4.3 PM-5 līdz PM-13: šī politika izpilda prasības attiecībā uz lomu dokumentēšanu, visas organizācijas risku lomām, konfigurācijas pārvaldības uzraudzību un integrāciju ar pamatdarbības funkcijām.

11.5 ES GDPR (2016/679)

11.5.1 Pants 5(1)(f): nosaka, ka personas dati jāaizsargā pret neatļautu vai nelikumīgu apstrādi. Šī politika nodrošina, ka personas, kas atbild par datu aizsardzību, ir skaidri noteiktas un uzraudzītas.

11.5.2 Pants 24: prasa atbilstošus organizatoriskos pasākumus, tostarp pārvaldības struktūras.

11.5.3 Pants 37: prasa datu aizsardzības speciālista (DPO) iecelšanu, kam jābūt atspoguļotam organizācijas pārvaldības ietvarā un atbildības reģistrā.

11.6 ES NIS2 direktīva (2022/2555)

11.6.1 Pants 21(2)(a): nosaka, ka subjekti ievieš politikas par risku analīzi un informācijas sistēmu drošību, tostarp lomām specifisku atbildību. Šī politika nosaka šādas lomas un to pārvaldības mehānismus.

11.7 ES DORA (2022/2554)

11.7.1 Pants 5 – IKT risku pārvaldības un iekšējās kontroles ietvars: prasa formāli noteikt IKT risku pārvaldības atbildību, lēmumu pieņemšanas lomas un ziņošanas kanālus. Šī politika nodrošina pamatu ar drošību saistīto lomu pārvaldībai IKT vidēs.

11.8 COBIT 2019

11.8.1 EDM01 – Nodrošināta pārvaldības ietvara izveide: šī politika nodrošina, ka ISMS ir skaidri noteikta pārvaldības struktūra, kas saskaņota ar organizācijas vajadzībām.

11.8.2 EDM02 – Nodrošināta ieguvumu sasniegšana: saskaņo uz lomām balstītas drošības darbības ar stratēģiskajiem un operacionālajiem mērķiem, nodrošinot atbildību un izmērāmus rezultātus.

11.8.3 APO01 – Pārvaldīts I&T pārvaldības ietvars un APO12 – Pārvaldīts risks: šī politika atbalsta strukturētu informācijas drošības lomu pārvaldību plašākā IT pārvaldības un risku ietvarā.

11.8.4 MEA01 – Uzraudzīt, izvērtēt un novērtēt veiktspēju: ietver pārskatīšanas mehānismus, lai pārliecinātos, ka pārvaldības lomas ir efektīvas, aktuālas un tiek piemērotas.