					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P06					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**

Saskaņojums ar standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	6.1., 8.32. un 10. punkts	Risku identificēšanas un pārvaldības pamatprasības, integrācija izmaiņu pārvaldībā, nepārtraukta pilnveide
ISO/IEC 27005:2024	Pilna riska dzīves cikla metodoloģija	Pilns risku pārvaldības process atbilstoši standartam
ISO 31000:2018	Risku pārvaldības principi un ietvars	Ietvarā pārņemti risku pārvaldības principi
NIST SP 800-30 Rev.1	SP 800-30, SP 800-39	Vadlīnijas un struktūra riska novērtēšanai, daudzlīmeņu risku pārvaldība
ES VDAR	24., 25. un 32. pants	Datu aizsardzības risku procesi un kontroles pasākumi
ES NIS2	21. panta 2. punkta a–d apakšpunkts	Riska novērtēšanas un drošības izvērtēšanas pienākumi
ES DORA	5. un 6. pants	IKT risku pārvaldība un darbības noturība
COBIT 2019	APO12, MEA	Risku pārvaldības struktūra un uzraudzība

1. Mērķis

1.1 Šī politika nosaka vienotu un formalizētu ietvaru informācijas drošības risku identificēšanai, analīzei, izvērtēšanai, apstrādei, uzraudzībai un pārskatīšanai visā organizācijā.

1.2 Tā nodrošina konsekventu uz risku balstītas pieejas piemērošanu, lai aizsargātu informācijas aktīvu konfidencialitāti, integritāti un pieejamību (CIA) saskaņā ar ISO/IEC 27001:2022 6.1. punktu un ISO 31000:2018.

1.3 Politika integrē informācijas drošības risku pārvaldību organizācijas lēmumu pieņemšanas procesos, lai nodrošinātu iekšējo stratēģisko mērķu sasniegšanu un ārējo normatīvo prasību izpildi.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām organizācijas struktūrvienībām, biznesa procesiem, sistēmām, personālu un sadarbības modeļiem ar trešajām pusēm, kas iesaistīti informācijas aktīvu apstrādē, izstrādē, glabāšanā vai pārvaldībā.

2.2 Piemērošanas joma aptver fiziskos, digitālos un mākoņvidē izvietotos aktīvus, tostarp strukturētus un nestrukturētus datus, lietojumprogrammas, infrastruktūru, tīklus un pakalpojumus.

2.3 Tā aptver informācijas drošības riskus stratēģiskajā, operacionālajā, projektu un tehniskajā līmenī un ir obligāta visiem darbiniekiem, līgumslēdzējiem un pakalpojumu sniedzējiem, kas iesaistīti ISMS darbībā.

2.4 Risku pārvaldība jāpiemēro šādos scenārijos:

2.4.1 jauna projekta vai sistēmas ieviešana;

2.4.1.1 būtiskas izmaiņas (piemēram, arhitektūrā, īpašumtiesībās, procesos);

2.4.1.2 piegādātāju piesaiste un līgumi ar trešajām pusēm;

2.4.1.3 reaģēšana uz incidentiem un pēcincidenta pārskatīšana;

2.4.1.4 periodiska organizācijas risku pārskatīšana vai auditi.

3. Mērķi

3.1 Izveidot un ieviest atkārtojamu, visas organizācijas mēroga risku pārvaldības procesu, kas balstīts uz ISO/IEC 27005 un ISO 31000 metodoloģiju.

3.2 Nodrošināt, ka riski tiek identificēti, analizēti, izvērtēti un apstrādāti, izmantojot strukturētas un izsekojamas metodes, tostarp nosakot atbildību par risku un sasaisti ar kontroles pasākumiem.

3.3 Uzturēt centralizētu un versiju kontrolētu risku reģistru un risku apstrādes plānu, kas atspoguļo aktuālo risku statusu, kontroles pasākumu pārklājumu un mazināšanas progresu.

3.4 Saskaņot lēmumus par risku ar dokumentētu riska apetīti un tolerances līmeņiem un nodrošināt informētu vadības lēmumu pieņemšanu par riska pieņemšanu, mazināšanu, pārnešanu vai izvairīšanos.

3.5 Nepārtraukti uzraudzīt risku tendences un nodrošināt risku apstrādes pasākumu efektivitāti, vienlaikus ļaujot proaktīvi veikt pielāgojumus atbilstoši apdraudējumu attīstībai vai izmaiņām biznesā.

4. Lomas un atbildība

4.1 Izpildvadība / valde

4.1.1 Apstiprina risku pārvaldības ietvaru un nosaka pieņemamo riska apetīti un tolerances sliekšņus.

4.1.2 Apstiprina riska apstrādes stratēģijas attiecībā uz atlikušajiem riskiem, kas pārsniedz toleranci.

4.1.3 Piešķir resursus un nodrošina uzraudzību risku pārvaldības programmas efektīvai darbībai.

4.2 Informācijas drošības pārvaldības sistēmas vadītājs / risku pārvaldnieks

4.2.1 Ir šīs politikas īpašnieks un nodrošina tās atbilstību ISO/IEC 27001 un ISO/IEC 27005 standartiem.

4.2.2 Vada organizācijas riska novērtēšanas procesu un uztur risku reģistru un risku apstrādes plānu.

4.2.3 Nodrošina periodisku pārskatīšanu un būtisko risku eskalāciju izpildvadībai vai Informācijas drošības vadības komitejai (ISSC).

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika un ar to saistītais ietvars jāpārskata reizi gadā vai:

9.1.1 pēc nozīmīga riska notikuma vai drošības incidenta;

9.1.2 pēc būtiskām organizatoriskām vai tehniskām izmaiņām;

9.1.3 reaģējot uz audita konstatējumiem vai jaunām normatīvajām prasībām.

9.2 Informācijas drošības pārvaldības sistēmas vadītājam, risku pārvaldniekam un atbilstības komandai kopīgi ir pienākums:

9.2.1 uzsākt pārskatīšanas ciklu;

9.2.2 apkopot ievaddatus no biznesa struktūrvienībām;

9.2.3 pēc vajadzības pārskatīt procedūras un sliekšņus.

9.3 Visi grozījumi:

9.3.1 jāpakļauj versiju kontrolei un jāreģistrē;

9.3.2 jāapstiprina izpildvadībai;

9.3.3 jākomunicē ieinteresētajām pusēm;

9.3.4 jāsaglabā audita repozitorijā vismaz 5 gadus.

10. Saistītās politikas un sasaistes

10.1 Šī politika ir savstarpēji saistīta ar šādām informācijas drošības politikām:

10.1.1 P1 – Informācijas drošības politika: nosaka kopējo drošības pārvaldības modeli, kura ietvaros tiek piemērota šī risku pārvaldības politika.

10.1.2 P2 – Pārvaldības lomu un atbildības politika: nosaka atbildīgos īpašniekus un pārvaldības līmeņus, uz kuriem atsaucas risku eskalācijas matrica.

10.1.3 P5 – Izmaiņu pārvaldības politika: nosaka pienākumu atkārtoti izvērtēt riskus infrastruktūras un organizatorisku izmaiņu gadījumā.

10.1.4 P13 – Datu klasifikācijas un marķēšanas politika: atbalsta ietekmes izvērtēšanu riska identificēšanas laikā.

10.1.5 P33 – Audita un atbilstības uzraudzības politika: validē politikas ievērošanu, tostarp risku reģistra pilnīgumu un riska apstrādes pierādījumus.

11. Atsauces standarti un ietvari

11.1 Šī politika ir tieši saskaņota ar turpmāk norādītajiem standartiem un ietvariem, lai nodrošinātu atbilstību starptautiski atzītai labai praksei un normatīvajām prasībām informācijas drošības risku pārvaldībā.

11.2 ISO/IEC 27001:

11.2.1 6.1. punkts: nosaka prasības risku un iespēju identificēšanai, tostarp pilnam informācijas drošības riska novērtēšanas un apstrādes dzīves ciklam. Šī politika ievieš 6.1.2. un 6.1.3. punkta prasības, nosakot strukturētu ietvaru riska identificēšanas, analīzes, izvērtēšanas, apstrādes un atlikušā riska pieņemšanas dokumentēšanai.

11.2.2 8.32. punkts: uz risku balstītas pieejas integrācija izmaiņu pārvaldības procesos nodrošina, ka visas būtiskās organizatoriskās izmaiņas izraisa formālu atkārtotu riska novērtēšanu.

11.2.3 10. punkts: nepārtraukta pilnveide tiek nodrošināta ar regulāru politikas pārskatīšanu, risku tendenču analīzi un SoA atjaunināšanu, kas balstīta uz risku izvērtēšanas atziņām.

11.3 ISO/IEC 27005:

11.3.1 Sniedz specializētas un detalizētas vadlīnijas informācijas drošības risku pārvaldībai. Šī politika ievieš pilnu ISO/IEC 27005 riska procesa modeli: konteksta noteikšana, riska identificēšana, riska analīze, riska izvērtēšana, riska apstrāde, riska pieņemšana, riska komunikācija, riska uzraudzība un pārskatīšana.

11.4 ISO 31000:

11.4.1 Šī politika integrē ISO 31000 principus, piemēram, vadības iesaisti, integrāciju lēmumu pieņemšanā un nepārtrauktu pilnveidi. Tā nodrošina, ka risku pārvaldība ir iekļauta organizācijas kultūrā un darbībā.

11.5 NIST SP 800-30 Rev.1:

11.5.1 Atbilst NIST vadlīnijām par riska novērtēšanas veikšanu, tostarp apdraudējumu identificēšanu, ievainojamību analīzi, iespējamības novērtēšanu un ietekmes noteikšanu. Šīs politikas struktūra atspoguļo NIST noteiktos riska novērtēšanas posmus un pielāgo tos gan tehniskajiem, gan biznesa procesiem.

11.6 NIST SP 800-39:

11.6.1 Atbalsta organizācijas līmeņa risku pārvaldību, uzsverot daudzlīmeņu risku pārvaldību organizācijas, misijas/biznesa procesa un informācijas sistēmas līmenī. Politika nodrošina, ka atbildība par risku ir skaidri noteikta visos līmeņos un ietver organizācijas līmeņa riska apstrādes stratēģijas.

11.7 ES VDAR:

11.7.1 24. pants: nosaka pienākumu ieviest atbilstošus tehniskos un organizatoriskos pasākumus, lai datu aizsardzības riski tiktu pienācīgi pārvaldīti; tas tiek nodrošināts ar šajā politikā noteikto strukturēto riska procesu.

11.7.2 25. pants: datu aizsardzība pēc projektēšanas un pēc noklusējuma atbilst riska apstrādes integrēšanai sistēmu un procesu izstrādē.

11.7.3 32. pants: nosaka uz risku balstītu pieeju drošības pasākumiem; to nodrošina uz ietekmi balstīta riska izvērtēšana un kontroles pasākumu atlase.

11.8 ES NIS2 direktīva:

11.8.1 21. panta 2. punkta a–d apakšpunkts: prasa subjektiem veikt riska novērtēšanu, ieviest politikas riska analīzei un nodrošināt samērīgus drošības pasākumus. Šī politika izpilda šos pienākumus, izmantojot nepārtrauktu riska dzīves cikla piemērošanu un dokumentētu pārvaldību.

11.9 ES DORA:

11.9.1 5. pants: nosaka prasību pēc dokumentēta IKT risku pārvaldības ietvara; to pilnībā aptver šīs politikas arhitektūra, tostarp SoA kartēšana un galvenie riska rādītāji.

11.9.2 6. pants: prasa integrēt risku pārvaldību darbības noturības stratēģijās; tas tiek nodrošināts ar eskalācijas matricām un kritisko aktīvu uzraudzību.

11.10 COBIT 2019:

11.10.1 APO12 – Risku pārvaldība: tieši atbilst organizācijas strukturētas risku pārvaldības pieejas izveidei, lomu piešķiršanai, riska apstrādes uzraudzībai un pārskatatbildības nodrošināšanai valdes līmenī.

11.10.2 MEA01 – Veiktspējas un atbilstības uzraudzība, izvērtēšana un novērtēšana: atspoguļojas šīs politikas fokusā uz tendenču analīzi, galveno riska rādītāju uzraudzību un audita atgriezeniskās saites integrēšanu nepārtrauktas pilnveides ciklos.