					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P01					Dokumenta nosaukums: **Informācijas drošības 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**

1. Mērķis

1.1 Šī politika nosaka organizācijas vispārējo apņemšanos nodrošināt informācijas drošību, ieviešot formālu informācijas drošības pārvaldības sistēmu (IDPS).

1.2 Tā nosaka stratēģisko virzību un pamatprasības visu informācijas aktīvu konfidencialitātes, integritātes, pieejamības un noturības aizsardzībai fiziskajā vidē, digitālajā vidē un mākoņvidē.

1.3 Šī politika izpilda ISO/IEC 27001:2022 5.1. un 5.2. punkta prasības, nosakot vadības nodomu, augstākās vadības apņemšanos un drošības darbību saskaņošanu ar organizācijas mērķiem.

1.4 Tā kalpo kā saistošs atsauces dokuments visām IDPS pakārtotajām politikām, standartiem un procedūrām un ir būtiska, lai nodrošinātu uz risku balstītu, uz atbilstību vērstu un nepārtraukti pilnveidojamu drošības vidi.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām personām, aktīviem un procesiem, kas noteikti IDPS piemērošanas jomā, tostarp:

2.1.1 visām uzņēmējdarbības vienībām, struktūrvienībām, meitas sabiedrībām un filiālēm;

2.1.2 darbiniekiem, darbuzņēmējiem, pagaidu personālam, konsultantiem un trešo pušu pakalpojumu sniedzējiem;

2.1.3 visiem datiem, informācijas sistēmām, lietojumprogrammām, infrastruktūrai un sakaru kanāliem;

2.1.4 visām fiziskajām, mākoņvides, attālinātajām un hibrīdajām vidēm, kurās tiek apstrādāti uzņēmuma dati vai nodrošināta piekļuve tiem.

2.2 Politika ir saistoša visām struktūrām, kas apstrādā organizācijas informāciju, un attiecas uz visiem informācijas aprites cikla posmiem — no izveides un pārsūtīšanas līdz glabāšanai un iznīcināšanai.

2.3 Jebkādi izņēmumi vai ierobežojumi šajā piemērošanas jomā ir jādokumentē IDPS piemērošanas jomas aprakstā un jāpamato ar izpildvadības formālu apstiprinājumu.

3. Mērķi

3.1 Izveidot IDPS, kas atbilst ISO/IEC 27001:2022 un atbalsta uz risku balstītu lēmumu pieņemšanu visā organizācijā.

3.2 Nodrošināt, ka konfidencialitātes, integritātes un pieejamības drošības principi ir iekļauti visās organizācijas darbībās, sistēmās un sadarbības attiecībās.

3.3 Nodrošināt normatīvo un līgumisko atbilstību, nosakot izmērāmus, politikā balstītus drošības mērķus un integrējot tos darbības procesos.

3.4 Samazināt informācijas drošības incidentu iespējamību un ietekmi, izmantojot efektīvus preventīvus, detektējošus un korektīvus kontroles pasākumus.

3.5 Veicināt nepārtrauktu informācijas drošības brieduma paaugstināšanu, izmantojot noteiktus veiktspējas rādītājus, auditu rezultātus un vadības pārskatīšanu.

3.6 Veicināt atbildības, informētības un noturības kultūru, kurā drošības pienākumi ir skaidri saprotami un tiek izpildīti visam personālam.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 Apstiprina un atbalsta informācijas drošības politiku un IDPS ietvaru.

4.1.2 Nodrošina drošības mērķu saskaņošanu ar organizācijas darbības stratēģiju.

4.1.3 Rāda personīgu piemēru un veicina spēcīgu informācijas drošības kultūru.

4.1.4 Pārskata un apstiprina būtiskas izmaiņas IDPS piemērošanas jomā, risku apstrādē un pārvaldības struktūrā.

4.2 Informācijas drošības vadītājs (CISO) / IDPS vadītājs

4.2.1 Atbild par IDPS darbību un uztur šo politiku atbilstoši ISO/IEC 27001 prasībām.

4.2.2 Vada risku izvērtēšanu, kontroles pasākumu ieviešanu un nepārtrauktas pilnveides procesus.

4.2.3 Nodrošina drošības darbību koordināciju starp funkcijām un pārrauga pakārtotās politikas.

4.2.4 Sniedz izpildvadībai pārskatus par IDPS statusu, incidentiem, auditu rezultātiem un rādītājiem.

4.2.5 Nodrošina, ka politikas pārskatīšana un aktualizēšana tiek veikta saskaņā ar šī dokumenta 9. sadaļu.

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

9. Pārskatīšanas un aktualizēšanas prasības

9.1 Pārskatīšanas biežums

9.1.1 Šī politika jāpārskata vismaz reizi gadā vai iestājoties kādam no šādiem ierosinātājiem:

9.1.1.1 būtiskas izmaiņas tiesiskajās, regulatīvajās vai līgumiskajās prasībās;

9.1.1.2 būtiskas izmaiņas organizācijas riska profilā;

9.1.1.3 iekšējo vai ārējo auditu rezultāti;

9.1.1.4 nozīmīgi incidenti vai kontroles pasākumu atteices.

9.2 Pārskatīšanas pilnvaras un process

9.2.1 Pārskatīšanas procesu vada CISO vai norīkots IDPS vadītājs.

9.2.2 Pārskatīšanas ievaddatos jāiekļauj:

9.2.2.1 iekšējā audita rezultāti;

9.2.2.2 risku izvērtēšanas tendences;

9.2.2.3 izmaiņas darbības procesos un tehnoloģijās;

9.2.2.4 sniegums attiecībā pret KPI un riska sliekšņiem.

9.2.3 Visiem atjauninājumiem:

9.2.3.1 jābūt versiju kontrolētiem un dokumentētiem;

9.2.3.2 jābūt apstiprinātiem izpildvadībā;

9.2.3.3 jābūt izplatītiem visām ietekmētajām pusēm pa oficiālajiem saziņas kanāliem;

9.2.3.4 jāizraisa nepieciešamie pakārtotās dokumentācijas un apmācību atjauninājumi.

10. Saistītās politikas un sasaistes

10.1 Šī pamatpolitika ir tieši saistīta ar šādām organizācijas drošības politikām un ietvariem:

10.1.1 P2 – Pārvaldības lomu un pienākumu politika: nosaka šajā dokumentā minēto pārvaldības struktūru un pilnvaru hierarhiju.

10.1.2 P3 – Pieļaujamās lietošanas politika: nosaka uzvedības prasības un pieļaujamu informācijas aktīvu lietošanu.

10.1.3 P4 – Piekļuves kontroles politika: operacionalizē no šīs pamatpolitikas izrietošos piekļuves kontroles pasākumus.

10.1.4 P6 – Risku pārvaldības politika: nodrošina uz risku balstītu kontekstu kontroles pasākumu izvēlei un atlikušā riska pieņemšanai.

10.1.5 P33 – Audita un atbilstības uzraudzības politika: nosaka, kā iekšējie pārliecības nodrošināšanas mehānismi apstiprina politikas ievērošanu.

10.2 Šīs savstarpējās saiknes nodrošina visaptverošu saskaņotību un izsekojamību visā IDPS un atbalsta vienotu risku un atbilstības pārvaldību.

11. Atsauces standarti un ietvari

11.1 Šī informācijas drošības politika ir formāli saskaņota ar šādiem standartiem un ietvariem, lai nodrošinātu pilnīgu atbilstību, gatavību auditam un regulatoriski pamatotu aizsardzību:

11.2 ISO/IEC 27001

11.2.1 5.1. punkts — līderība un apņemšanās: šī politika apliecina augstākās vadības apņemšanos informācijas drošības jomā un nosaka IDPS pienākumus un resursu piešķiršanu.

11.2.2 5.2. punkts — informācijas drošības politika: šis dokuments kalpo kā organizācijas formālā drošības politika, kas ir saskaņota ar noteiktajiem drošības mērķiem, darbības stratēģiju un ISO/IEC 27001 prasībām.

11.2.3 6.1. punkts — darbības risku un iespēju novēršanai: šajā politikā ietvertā uz risku balstītā pieeja nodrošina, ka drošības resursi tiek piemēroti samērīgi apdraudējumiem.

11.2.4 9.2. punkts — iekšējais audits un 10. punkts — pilnveide: šī politika ir integrēta organizācijas nepārtrauktas pilnveides ciklā un ir pakļauta iekšējā audita apstiprinājumam.

11.2.5 ISO/IEC 27002:2022 — kontroles pasākums 5.1: nosaka vadlīnijas drošības politiku izveidei un uzturēšanai. Šī politika atspoguļo ISO/IEC 27002 ieteikumus attiecībā uz hierarhisku dokumentāciju, pārskatīšanas cikliem un piemērojamību.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 (drošības plānošanas politika un procedūras): šī politika izpilda prasību izstrādāt, izplatīt un pārskatīt formālu, visā organizācijā piemērojamu informācijas drošības politiku.

11.3.2 PM-1 līdz PM-5: aptver programmas līmeņa pārvaldību, tostarp informācijas drošības lomas, resursu piešķiršanu, risku stratēģiju un drošības plānošanas integrāciju organizācijas darbībā.

11.4 ES GDPR (2016/679)

11.4.1 5. panta 2. punkts: nostiprina pārskatatbildības principu. Šī politika nosaka atbildīgās personas un izsekojamas ieviešanas darbības.

11.4.2 24. pants: prasa ieviest tehniskos un organizatoriskos pasākumus, tostarp ar risku saskaņotas politikas.

11.4.3 32. pants: atbalsta piemērotu pasākumu ieviešanu personas datu drošības nodrošināšanai visā to aprites ciklā.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 21. panta 2. punkta a) apakšpunkts: uzliek pienākumu subjektiem ieviest dokumentētu drošības politiku, kas aptver risku pārvaldību un pārvaldību. Šī politika izpilda šo prasību un atbalsta plašāku kiberdrošības gatavību un kritiskās infrastruktūras aizsardzību.

11.6 ES DORA (2022/2554)

11.6.1 5. panta 2. punkts: prasa dokumentētu iekšējās kontroles ietvaru IKT risku pārvaldībai. Šī politika atbalsta finanšu sektora atbilstību, nosakot lomas, kontroles pasākumus un pārraudzības funkcijas, kas atbilst DORA pārvaldības prasībām.

11.7 COBIT 2019

11.7.1 EDM01 — pārvaldības ietvara noteikšana: šī politika atbalsta organizācijas pārvaldību, nosakot IDPS lomas, vadības apņemšanos un stratēģiskos mērķus.

11.7.2 APO01 — pārvaldības ietvars: atbalsta strukturētas IDPS izveidi un darbību.

11.7.3 APO12 — risku pārvaldība: nodrošina pamatu informācijas drošības risku pārvaldībai.

11.7.4 MEA01/MEA03 — uzraudzīt, izvērtēt un novērtēt: stiprina nepārtrauktu veiktspējas izvērtēšanu un iekšējās kontroles uzraudzību, nodrošinot politikas ievērošanu.