					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P01S					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**

Saskaņojums ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkti 5.1, 5.2, 5.3, 6.1, 6.2, 8	Nosaka vadības apņemšanos, politikas prasības, lomu piešķiršanu, risku izvērtēšanu un darbības kontroles pasākumus
ISO/IEC 27002:2022	Kontroles pasākumi 5.1–5.5	Nosaka dokumentētas informācijas drošības politikas izveidi, lomu piešķiršanu, pienākumu nodalīšanu un vadības atbildību
NIST SP 800-53 Rev.5	PM-1, PL-1, CA-1, AC-1	Nosaka prasības drošības programmas plānam, drošības plānošanas politikai, izvērtēšanai un autorizācijai, kā arī piekļuves kontrolei
GDPR (ES) 2016/679	5. panta 2. punkts, 32. pants	Pārskatatbildības princips un apstrādes drošības pasākumi, jo īpaši attiecībā uz dokumentētām lomām
NIS2 direktīva (ES) 2022/2555	21. panta 2. punkta a) apakšpunkts	Pieprasa kiberrisku pārvaldības pasākumus, lomu noteikšanu un atbildību
DORA (ES) 2022/2554	9. pants, 10. pants	Pieprasa lomu piešķiršanu IKT risku pārvaldībai un darbības nepārtrauktībai
COBIT 2019	EDM03, APO13, DSS05	Nodrošina risku optimizāciju, drošības pārvaldību un drošības pakalpojumu pārvaldību, izmantojot skaidru lomu piešķiršanu

1. Mērķis

1.1 Šī politika apliecina organizācijas apņemšanos aizsargāt klientu un uzņēmuma informāciju, skaidri nosakot atbildību un praktiskus drošības pasākumus, kas ir piemēroti organizācijām bez specializētas IT komandas.

1.2 Tā nodrošina, ka visi darbinieki, darbuzņēmēji un pakalpojumu sniedzēji ievēro saistošās prasības, lai nodrošinātu pilnīgu atbilstību ISO/IEC 27001 sertifikācijas prasībām.

1.3 Šī politika ļauj organizācijai stiprināt klientu uzticēšanos, skaidri demonstrējot, kā viņu informācija tiek aizsargāta, izmantojot noteiktu atbildību, strukturētus procesus un skaidru pārskatatbildību.

2. Darbības joma

2.1 Šī politika attiecas uz visām personām, kuras piekļūst organizācijas datiem un sistēmām vai tās pārvalda, tostarp:

2.1.1 uzņēmuma īpašniekiem un izpilddirektoru

2.1.2 darbiniekiem, darbuzņēmējiem un praktikantiem

2.1.3 ārējiem IT pakalpojumu sniedzējiem vai konsultantiem

2.2 Tā aptver visus informācijas, sistēmu un pakalpojumu veidus, tostarp:

2.2.1 uzņēmuma ierakstus, klientu datus, paroles un e-pastus

2.2.2 IT aparatūru, piemēram, klēpjdatorus un tālruņus

2.2.3 mākoņpakalpojumus, ko izmanto failu glabāšanai, saziņai vai finanšu pārvaldībai

2.2.4 fiziskus dokumentus, kas tiek glabāti biroja telpās

2.3 Politika ir piemērojama visās darba vidēs — birojā, attālināti un mākoņvidē — un attiecas uz visām ierīcēm un programmatūru, ko izmanto uzņēmuma informācijas apstrādei vai glabāšanai.

3. Mērķi

3.1 Skaidri noteikt atbildību: ir jānodrošina, ka par informācijas drošību vienmēr ir noteikta atbildīgā persona. Parasti tas ir izpilddirektors vai persona, kuru viņš ir oficiāli pilnvarojis.

3.2 Aizsargāt klientu un uzņēmuma informāciju: ir jānodrošina uzticami un konsekventi aizsardzības pasākumi, lai novērstu sensitīvu datu, tostarp klientu un finanšu ierakstu, neatbilstošu izmantošanu, zudumu vai zādzību.

3.3 Atbalstīt ISO/IEC 27001 sertifikāciju: ir jānodrošina, ka organizācija var pierādīt pilnīgu atbilstību ISO/IEC 27001 prasībām, saglabājot gatavību auditam un iespēju saņemt sertifikāciju bez sarežģītas infrastruktūras ieviešanas.

3.4 Integrēt drošību uzņēmuma darbībā: informācijas drošība ir jāintegrē ikdienas uzdevumos un lēmumu pieņemšanā visā organizācijā.

3.5 Veidot izpratni un drošības kultūru: ir jānodrošina, ka ikviens darbinieks izprot un ievēro drošības praksi, piemēram, izmanto drošas paroles un ziņo par aizdomīgām darbībām.

4. Lomas un atbildība

4.1 Izpilddirektors vai uzņēmuma īpašnieks

4.1.1 Ir pilnībā atbildīgs par informācijas drošību.

4.1.2 Apstiprina un uztur šo politiku.

4.1.3 Nodrošina, ka visi būtiskie drošības uzdevumi tiek vai nu veikti tieši, vai rakstiski deleģēti.

4.1.4 Pārliecinās, ka visi deleģētie drošības uzdevumi, piemēram, piekļuves pārvaldība vai reaģēšana uz incidentiem, tiek veikti efektīvi.

4.1.5 Ir noklusējuma kontaktpersona visos iekšējos un ārējos drošības jautājumos, tostarp saistībā ar auditiem un klientu pieprasījumiem.

4.1.6 Ikgadējās pārskatīšanas laikā uzrauga progresu attiecībā pret šiem mērķiem. Mērķiem, kur iespējams, jābūt izmērāmiem, piemēram, apmācīto darbinieku īpatsvars, ziņoto incidentu skaits u. c., un tie jāpārskata, ņemot vērā drošības konstatējumus un risku izmaiņas.

4.2 Norīkots darbinieks (ja piemērojams)

4.2.1 Var atbalstīt izpilddirektoru, veicot ikdienas uzdevumus, piemēram, izveidojot lietotāju kontus, atņemot piekļuvi darbiniekiem, kuri izbeidz darba attiecības, vai koordinējot sadarbību ar IT pakalpojumu sniedzēju.

4.2.2 Tam ir jābūt oficiāli norīkotam, un tam ir jābūt pietiekamām pilnvarām un rīkiem uzdevumu izpildei.

4.2.3 Ziņo izpilddirektoram par visām konstatētajām problēmām.

[... 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 Šī politika GM ir jāpārskata vismaz reizi gadā, lai nodrošinātu nepārtrauktu atbilstību ISO/IEC 27001 sertifikācijas prasībām, normatīvo prasību izmaiņām, piemēram, GDPR, NIS2 un DORA, kā arī mainīgajām uzņēmuma vajadzībām.

9.2 Ārpuskārtas pārskatīšana

9.2.1 Papildu pārskatīšana ir jāveic, ja notiek būtiskas izmaiņas, piemēram:

9.2.1.1 nozīmīgi drošības incidenti vai pārkāpumi

9.2.1.2 jaunu uzņēmuma procesu vai tehnoloģiju ieviešana, piemēram, jauna programmatūra, attālinātā darba platformas vai mākoņpakalpojumi

9.2.1.3 izmaiņas tiesiskajās vai regulatīvajās prasībās, kas ietekmē rīcību ar informāciju

9.3 Izmaiņu dokumentēšana

9.3.1 Visas politikas pārskatīšanas un izmaiņas ir formāli jādokumentē, skaidri norādot datumu, izmaiņu būtību un GM apstiprinājumu.

9.3.2 Politikas versiju vēsture ir droši jāuztur, lai auditu laikā varētu pierādīt politikas attīstību un atbilstību.

9.4 Paziņošana par atjauninājumiem

9.4.1 Par jebkurām izmaiņām šajā politikā nekavējoties jāinformē visi darbinieki, darbuzņēmēji un attiecīgās trešās personas.

9.4.2 Atjauninātajām politikas versijām jābūt viegli pieejamām visam skartajam personālam, piemēram, koplietotā elektroniskā formā vai fiziski izvietotām darba vietā.

10. Saistītās politikas un savstarpējā sasaiste

10.1 Šī politika ir cieši saistīta ar citām organizācijas SME politiku kopuma politikām, jo īpaši:

10.1.1 P2S – Pārvaldības lomu un atbildības politika: precizē drošības pienākumu un atbildības sadalījumu.

10.1.2 P4S – Piekļuves kontroles politika: nosaka drošu piekļuves pārvaldību uzņēmuma informācijai.

10.1.3 P8S – Informācijas drošības izpratnes un apmācību politika: nosaka būtiskās vadlīnijas darbinieku apmācībai un izpratnes veicināšanai.

10.1.4 P17S – Datu aizsardzības un privātuma politika: nodrošina atbilstību GDPR un citiem datu aizsardzības tiesību aktiem.

10.1.5 P30S – Reaģēšanas uz incidentiem politika: apraksta detalizētas darbības, kas jāveic, reaģējot uz drošības incidentiem.

10.2 Šīs saistītās politikas sniedz skaidras darbības vadlīnijas, un tās jāievieš kopumā, lai nodrošinātu pilnīgu atbilstību ISO/IEC 27001 sertifikācijas prasībām.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 Punkts 5.1 – Līderība un apņemšanās: nosaka augstākās vadības apņemšanos un atbildību par informācijas drošības efektivitāti organizācijā.

11.1.2 Punkts 5.2 – Informācijas drošības politika: nosaka skaidru, dokumentētu politiku, kas saskaņota ar organizācijas stratēģiju un atbilstības prasībām.

11.1.3 Punkts 5.3 – Organizatoriskās lomas un atbildība: nosaka skaidru informācijas drošības pienākumu sadalījumu visā organizācijā, kas ir būtisks efektīvai pārvaldībai un atbilstībai audita prasībām.

11.1.4 Punkts 6.1 – Darbības risku un iespēju novēršanai: nodrošina, ka informācijas drošības riski tiek sistemātiski identificēti, izvērtēti un apstrādāti.

11.1.5 Punkts 8.1 – Darbības plānošana un kontrole: nosaka, ka organizācijai jāplāno un jāievieš procesi, kas nepieciešami informācijas drošības mērķu sasniegšanai un saistīto risku efektīvai pārvaldībai.

11.2 ISO/IEC 27002:2022 kontroles pasākumi 5.1–5.5

11.2.1 Pielikuma A kontroles pasākums 5.1 – Informācijas drošības politikas: nosaka dokumentētu informācijas drošības politiku izveidi un paziņošanu.

11.2.2 Pielikuma A kontroles pasākums 5.2 – Informācijas drošības lomas: precizē un formāli piešķir informācijas drošības lomas un atbildību attiecīgajām pusēm.

11.2.3 Pielikuma A kontroles pasākums 5.3 – Pienākumu nodalīšana: nosaka skaidru pienākumu nošķiršanu, lai mazinātu interešu konfliktu un krāpšanas risku sensitīvas informācijas pārvaldībā.

11.2.4 Pielikuma A kontroles pasākums 5.4 – Vadības atbildība: nosaka, ka vadībai ir jāpierāda apņemšanās nodrošināt informācijas drošību, īstenojot aktīvu uzraudzību un resursu piešķiršanu.

11.2.5 Pielikuma A kontroles pasākums 5.5 – Saziņa ar kompetentajām iestādēm: pastiprina nepieciešamību pēc skaidri dokumentētām informācijas drošības politikām, lomām, atbildības un pārvaldības struktūrām, nodrošinot konsekventu pārvaldību un audita pēdu visā organizācijā.

11.3 NIST SP 800-53 Rev.5

11.3.1 PM-1 – Informācijas drošības programmas plāns: nosaka dokumentētu informācijas drošības pārvaldības stratēģiju un politiku, nodrošinot ietvaru konsekventai ieviešanai un pārvaldībai.

11.3.2 PL-1 – Drošības plānošanas politika: nosaka organizācijas mēroga drošības plānošanas politiku, lai virzītu drošu darbību un informācijas drošības aktivitāšu stratēģisko saskaņotību.

11.3.3 CA-1 – Drošības izvērtēšanas un autorizācijas politika: nosaka skaidri definētas izvērtēšanas un autorizācijas lomas, lai nodrošinātu nepārtrauktu efektivitāti un atbilstību informācijas drošības prasībām.

11.3.4 AC-1 – Piekļuves kontroles politika: nosaka, ka organizācijām skaidri jādefinē, jādokumentē un jānodrošina piekļuves pārvaldības prakses un atbildības ievērošana.

11.4 GDPR (ES) 2016/679

11.4.1 5. panta 2. punkts – Pārskatatbildības princips: nosaka, ka organizācijām jāpierāda atbilstība datu aizsardzības principiem, tostarp izmantojot dokumentētas lomas un politikas datu aizsardzības pienākumu izpildei.

11.4.2 32. pants – Apstrādes drošība: nosaka atbilstošu tehnisko un organizatorisko pasākumu ieviešanu, tostarp skaidri noteiktu drošības atbildību, lai aizsargātu personas datus pret pārkāpumiem un neatļautu piekļuvi.

11.5 NIS2 direktīva (ES) 2022/2555

11.5.1 21. panta 2. punkta a) apakšpunkts – Risku pārvaldības pasākumi: nosaka skaidru pārvaldības kārtību, tostarp noteiktas lomas un atbildību par informācijas drošību, kas ir būtiska efektīvai kiberrisku pārvaldībai.

11.6 DORA (ES) 2022/2554

11.6.1 9. pants – IKT risku pārvaldība: nosaka, ka organizācijām skaidri jāpiešķir lomas un atbildība saistībā ar IKT risku pārvaldību, stiprinot noturību un gatavību darbības nepārtrauktības nodrošināšanai.

11.6.2 10. pants – IKT darbības nepārtrauktība: nosaka skaidru pārskatatbildību un strukturētas lomas IKT noturības un nepārtrauktības uzturēšanai, nodrošinot organizāciju spēju uzticami reaģēt uz traucējumiem.

11.7 COBIT 2019

11.7.1 EDM03 – Risku optimizācijas nodrošināšana: uzsver skaidri noteiktu pārskatatbildību un lomas organizācijas risku pārvaldībā, nodrošinot stingru pārvaldību un efektīvu informācijas drošības risku uzraudzību.

11.7.2 APO13 – Drošības pārvaldība: nosaka, ka organizācijām skaidri jāizveido un jāpaziņo drošības pārvaldības pienākumi, nodrošinot saskaņotību ar uzņēmuma mērķiem un regulatīvajām prasībām.

11.7.3 DSS05 – Drošības pakalpojumu pārvaldība: paredz strukturētas lomas un skaidru atbildību drošības pakalpojumu pārvaldībā, nodrošinot konsekventu ieviešanu un atbilstības pārbaudi.