					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P37S					Dokumenta nosaukums: **Juridiskās un regulatīvās atbilstības 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**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	Punkti 5.1, 6.1, 6.2, 8	
ISO/IEC 27002:2022	5. kontrole	
NIST SP 800-53 Rev.5	PL-1, PL-2, PM-1, CA-1, AU-1	
ES VDAR	Panti 5, 6, 32, 33	
ES NIS2	Panti 21(2)(a), 21(2)(f), 23	
ES DORA	Panti 5(2), 9(1), 17	
COBIT 2019	APO12, APO13, DSS01	

1. Mērķis

1.1 Šī politika nosaka organizācijas pieeju juridisko, regulatīvo un līgumisko pienākumu identificēšanai, izpildei un atbilstības apliecināšanai.

1.2 Tā nosaka skaidrus pienākumus un praktiskus pasākumus, lai palīdzētu uzņēmumam izpildīt atbilstības prasības, tostarp datu aizsardzības prasības, kiberdrošības ietvarus, klientu līgumsaistības un sertifikācijas standartus.

1.3 Tā nodrošina, ka arī bez īpaši izveidotas atbilstības komandas uzņēmums var uzturēt tiesiski pamatotu darbību, pienācīgi reaģēt uz incidentiem un saglabāt gatavību auditam.

1.4 Šī politika ir būtiska ISO/IEC 27001:2022 sertifikācijas nodrošināšanai un ārējo pušu, tostarp klientu, regulatoru un partneru, prasību izpildei.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem darbiniekiem, līgumslēdzējiem, ārštata darbiniekiem un trešo pušu piegādātājiem;

2.1.2 visiem pakalpojumiem, darbībām, sistēmām un datu apstrādes darbībām, kurās organizācijai ir jāizpilda juridiskās vai līgumiskās prasības;

2.1.3 visām atrašanās vietām un ierīcēm, ko izmanto uzņēmuma informācijas apstrādei, neatkarīgi no tā, vai tās atrodas birojā, tiek izmantotas attālināti vai ir izvietotas mākoņvidē.

2.2 Politika aptver:

2.2.1 datu aizsardzības tiesību aktus, piemēram, ES VDAR;

2.2.2 kiberdrošības regulējumu, piemēram, ES NIS2;

2.2.3 nozarei specifiskus pienākumus, ja tādi ir piemērojami;

2.2.4 klientu līgumus, konfidencialitātes līgumus un audita klauzulas;

2.2.5 brīvprātīgās sertifikācijas (piemēram, ISO 27001) un iekšējās politikas, kuru ievērošana ir nepieciešama atbilstības nodrošināšanai.

3. Mērķi

3.1 Noteikt pārskatatbildību: piešķirt skaidru atbildību par juridisko, regulatīvo un līgumisko pienākumu uzraudzību, aktualizēšanu un piemērošanu.

3.2 Aizsargāt uzņēmumu: samazināt juridisku pārkāpumu, naudas sodu, datu aizsardzības pārkāpumu un reputācijas kaitējuma risku.

3.3 Nodrošināt gatavību auditam: uzturēt pārbaudāmus ierakstus, kas apliecina, kā organizācija izpilda savus atbilstības pienākumus.

3.4 Atbalstīt politiku integrāciju: nodrošināt, ka juridiskie un regulatīvie pienākumi tiek konsekventi ieviesti visās politikās un procesos.

3.5 Pārvaldīt izņēmumus pārredzami: nodrošināt, ka jebkuri atbilstības izņēmumi ir dokumentēti, pamatoti un apstiprināti, lai mazinātu atbildības risku.

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 Uzņemas vispārējo pārskatatbildību par organizācijas juridisko un regulatīvo atbilstību.

4.1.2 Uztur atbilstības reģistru un nodrošina tā aktualitāti.

4.1.3 Pārskata klientu līgumus un nodrošina, ka specifiskie pienākumi tiek uzskaitīti un piemēroti.

4.1.4 Apstiprina izņēmumus no atbilstības prasībām tikai tad, ja tie ir tiesiski pamatoti un ir ieviesti kompensējoši kontroles pasākumi.

4.2 Ārējie konsultanti (piemēram, juridiskie, IT vai atbilstības konsultanti)

4.2.1 Atbalsta GM, identificējot piemērojamos tiesību aktus, sertifikācijas prasības un pienākumus (piemēram, VDAR, NIS2, ISO 27001).

4.2.2 Sniedz ieteikumus par jauna regulējuma vai spēkā esošo tiesību aktu izmaiņu interpretāciju.

4.2.3 Vajadzības gadījumā var palīdzēt politiku atjaunināšanā, auditos vai reaģēšanā uz pārkāpumiem, ja tiem ir juridiska ietekme.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Plānotā ikgadējā pārskatīšana

9.1.1 Šī politika GM jāpārskata ik pēc 12 mēnešiem.

9.1.2 Pārskatīšanā jāapstiprina:

9.1.2.1 atbilstība aktuālajam juridiskajam un līgumiskajam kontekstam;

9.1.2.2 korekts klientu vienošanos un pakalpojumu pienākumu atspoguļojums;

9.1.2.3 saskaņotība ar atbilstības reģistru un citām politikām.

9.2 Notikumu izraisīti atjauninājumi

9.2.1 Nekavējoša pārskatīšana ir nepieciešama, ja:

9.2.1.1 kļūst piemērojams jauns tiesību akts vai regulējums (piemēram, jauna datu aizsardzības prasība);

9.2.1.2 klients savā līgumā iekļauj sarežģītus atbilstības noteikumus;

9.2.1.3 notiek pārkāpums vai neatbilstības incidents;

9.2.1.4 uzņēmums paplašina darbību regulētā tirgū vai nozarē.

9.3 Atjauninājumu apstiprināšana un versiju kontrole

9.3.1 Visi atjauninājumi jādokumentē, jāversē un jāapstiprina GM.

9.3.2 Vēsturiskās versijas jāsaglabā audita un juridiskiem mērķiem.

9.4 Izmaiņu komunikācija

9.4.1 Personāls un līgumslēdzēji jāinformē par politikas grozījumiem 5 darbdienu laikā pēc apstiprināšanas.

9.4.2 Arī skartajiem piegādātājiem pirms pakalpojumu sniegšanas turpināšanas jāapliecina atjaunināto noteikumu pieņemšana.

10. Saistītās politikas un sasaiste

10.1 Šo politiku atbalsta un palīdz ieviest šādas SME politikas:

10.1.1 P3S – Pieņemamas lietošanas politika: novērš rīcību, kas var pārkāpt juridiskos vai līgumiskos noteikumus (piemēram, neatļautu failu kopīgošanu).

10.1.2 P8S – Informācijas drošības informētības un apmācības politika: izglīto personālu par atbilstības pienākumiem un to, kā izvairīties no pārkāpumiem.

10.1.3 P14S – Datu uzglabāšanas politika un Datu likvidēšanas politika: nodrošina likumīgu datu apstrādes praksi visā datu dzīves ciklā.

10.1.4 P17S – Datu aizsardzības un privātuma politika: nodrošina VDAR un klientu datu apstrādes prasību izpildi.

10.1.5 P30S – Incidentu reaģēšanas politika: nosaka, kā reaģēt uz datu aizsardzības pārkāpumiem vai atbilstības neizpildi, tostarp paziņošanas termiņus.

10.1.6 P36S – Sociālo mediju un ārējās komunikācijas politika: nodrošina, ka publiskā komunikācija nepārkāpj juridiskos vai regulatīvos pienākumus.

10.2 Katra saistītā politika nodrošina daļu no juridiskās atbilstības ietvara, un tās jāpiemēro savstarpēji saskaņoti.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 Punkts 6.1 – darbības risku un iespēju novēršanai: ietver atbilstības riskus.

11.1.2 Punkts 8.1 – darbības plānošana un kontrole: nosaka procesu izpildi, lai nodrošinātu atbilstību juridiskajām un līgumiskajām prasībām.

11.2 ISO/IEC 27002

11.2.1 5.36. kontrole – sniedz norādes organizācijai par pienākumu uzskaites uzturēšanu un atbilstošas reaģēšanas nodrošināšanu uz juridiskajām un regulatīvajām prasībām.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Politika un procedūras: nosaka formālas atbilstības politikas nepieciešamību.

11.3.2 PM-1 – Informācijas drošības programmas plāns: nosaka juridiskās atbilstības integrēšanu drošības plānošanā.

11.3.3 CA-1 – izvērtēšana, autorizācija un uzraudzība.

11.3.4 AU-1 – Audita politika: nosaka atbilstības pierādījumu uzturēšanu.

11.4 ES VDAR

11.4.1 5. pants – datu apstrādes principi, tostarp pārskatatbildība.

11.4.2 6. pants – apstrādes tiesiskais pamats.

11.4.3 32. pants – apstrādes drošība.

11.4.4 33. pants – paziņošana par pārkāpumu 72 stundu laikā.

11.5 ES NIS2 direktīva

11.5.1 21(2)(a) un (f) pants – iekšējās politikas risku un regulatīvās kontroles nodrošināšanai.

11.5.2 23. pants – ieviešana un sankcijas par atbilstības neizpildi.

11.6 ES DORA regula

11.6.1 5(2) pants – IKT risku pārvaldības pārraudzība.

11.6.2 9(1) pants – iekšējā atbilstības pārvaldība.

11.6.3 17. pants – līgumiskās attiecības ar IKT pakalpojumu sniedzējiem.

11.7 COBIT 2019

11.7.1 APO12 – Pārvaldīts risks: nodrošina, ka atbilstības riski tiek uzskaitīti un novērsti.

11.7.2 APO13 – Pārvaldīta drošība: aptver uz risku balstītu regulatīvās un līgumiskās atbilstības piemērošanu.

11.7.3 DSS01 – Pārvaldītas operācijas: nosaka darbības gatavību juridisko pienākumu izpildei.