					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P37					Dokumenta nosaukums: **Tiesiskās 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**

Juridiskais paziņojums (autortiesības un lietošanas ierobežojumi)
(C) 2025 Clarysec LLC. All rights reserved.

Šis dokuments ir Clarysec LLC intelektuālais īpašums. Nevienu šī dokumenta daļu nedrīkst kopēt, atkārtoti izmantot, izplatīt vai grozīt komerciāliem vai ieviešanas nolūkiem bez iepriekšējas skaidras rakstiskas atļaujas.
Neautorizēta lietošana ir stingri aizliegta un var izraisīt tiesvedību.
Par licencēšanu sazinieties: info@clarysec.com

1. Mērķis

1.1 Šī politika nosaka obligātu ietvaru visu tiesisko, regulatīvo un līgumisko pienākumu identificēšanai, pārvaldībai un atbilstības nodrošināšanai, kas attiecas uz organizācijas informācijas drošību, datu aizsardzību un darbības funkcijām.

1.2 Tās mērķis ir novērst neatbilstību, kas var izraisīt naudas sodus, juridisko atbildību, darbības traucējumus, reputācijas kaitējumu vai regulatora noteiktus pasākumus.

1.3 Šī politika atbalsta atbilstības prasību integrēšanu pārvaldībā, risku pārvaldībā, darbības procesos, projektu dzīves ciklā un sistēmu izstrādē.

1.4 Tā nodrošina, ka visi attiecīgie pienākumi dažādās jurisdikcijās, nozarēs un regulatīvās piemērošanas jomās organizācijā tiek skaidri dokumentēti, izvērtēti, uzraudzīti un ieviesti.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām struktūrvienībām, funkcijām, biznesa vienībām un personām, kas rīkojas organizācijas vārdā, tai skaitā:

2.1.1 pastāvīgajiem un pagaidu darbiniekiem;

2.1.2 līgumdarbiniekiem, konsultantiem un praktikantiem;

2.1.3 trešo pušu piegādātājiem, apstrādātājiem vai partneriem, kas apstrādā organizācijas datus, izmanto tās sistēmas vai uzņemas regulatīvus pienākumus;

2.1.4 jebkuriem biznesa procesiem, projektiem vai iniciatīvām, uz kurām attiecas tiesiskā vai regulatīvā kontrole.

2.2 Šīs politikas aptvertās atbilstības jomas ietver, bet neaprobežojas ar:

2.2.1 informācijas drošības un kiberdrošības pienākumiem (piemēram, ISO/IEC 27001, NIS2, DORA);

2.2.2 datu aizsardzības un privātuma tiesību aktiem (piemēram, GDPR, nozarei specifiskiem privātuma normatīvajiem aktiem);

2.2.3 nozaru regulējumu (piemēram, finanšu, medicīnas, autobūves un aizsardzības jomā);

2.2.4 līgumiskajiem pienākumiem, kas izriet no konfidencialitātes līgumiem, pakalpojumu līmeņa vienošanām (SLA) vai trešo pušu apstrādes līgumiem;

2.2.5 tiesiskajām prasībām saistībā ar ziņošanu par incidentiem, sadarbību ar tiesībaizsardzības iestādēm un starptautisku datu pārsūtīšanu.

3. Mērķi

3.1 Nodrošināt, ka visi piemērojamie tiesību akti, regulējums, standarti un līgumiskie pienākumi visā organizācijā tiek identificēti, dokumentēti, interpretēti un ieviesti.

3.2 Integrēt tiesiskās un regulatīvās prasības organizācijas informācijas drošības pārvaldības sistēmā, risku pārvaldības procesos, piegādātāju līgumos un produktu/pakalpojumu izstrādē.

3.3 Nodrošināt mehānismu proaktīvai regulatīvo izmaiņu uzraudzībai un attiecīgai kontroles pasākumu un dokumentācijas atjaunināšanai.

3.4 Noteikt skaidru pārskatatbildību par atbilstības pārraudzību, pārkāpumu eskalāciju, izņēmumu pārvaldību un ārējo ziņošanu.

3.5 Nodrošināt organizācijas tiesiskā un regulatīvā stāvokļa auditējamību un spēju to pamatot inspekciju, izmeklēšanu vai sertifikācijas pārskatīšanas laikā.

4. Lomas un pienākumi

4.1 Izpildvadība

4.1.1 Uzņemas stratēģisko pārskatatbildību par tiesisko un regulatīvo atbilstību visā organizācijā.

4.1.2 Pārskata un apstiprina augsta riska atbilstības lēmumus, tai skaitā riska pieņemšanu un juridiskus strīdus.

4.2 Juridiskās un atbilstības funkcijas speciālists / galvenais juridiskais padomnieks / juridiskais konsultants

4.2.1 Uztur Atbilstības pienākumu reģistru, kurā uzskaitīti visi piemērojamie tiesību akti, standarti, sertifikācijas un līgumu klauzulas.

4.2.2 Veic tiesiskās ietekmes izvērtēšanu jauniem pakalpojumiem, tirgiem vai datu plūsmām.

4.2.3 Sniedz autoritatīvu tiesību aktu un standartu interpretāciju.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ikgadēja politikas pārskatīšana

9.1.1 Šī politika jāpārskata vismaz vienu reizi kalendārajā gadā, lai:

9.1.1.1 nodrošinātu pastāvīgu atbilstību aktualizētiem tiesību aktiem, nozares standartiem un regulatīvajiem ietvariem;

9.1.1.2 apstiprinātu darbības efektivitāti, pamatojoties uz audita konstatējumiem un incidentu vēsturi;

9.1.1.3 atspoguļotu organizatoriskas izmaiņas (piemēram, jaunas jurisdikcijas, sistēmas vai darbības virzienus).

9.2 Pārskatīšana pēc ierosinātājiem

9.2.1 Starpposma pārskatīšana jāuzsāk, ja:

9.2.2 tiek pieņemta vai atjaunināta jauna tiesiskā vai regulatīvā prasība;

9.2.3 atbilstības incidents vai audits atklāj politikas nepilnības;

9.2.4 organizācija uzsāk darbību jaunā tirgū vai pakalpojumu jomā, uz kuru attiecas atšķirīgi atbilstības ietvari;

9.2.5 piemērošanas tendences vai regulatoru vadlīnijas norāda uz riska stāvokļa izmaiņām.

9.3 Īpašumtiesības un apstiprināšana

9.3.1 Juridiskā struktūrvienība un juridiskās un atbilstības funkcijas speciālists ir kopīgi pārskatatbildīgi par pārskatīšanas procesa koordinēšanu.

9.3.2 Politikas galīgie grozījumi jāapstiprina izpildvadībai un jāreģistrē politikas grozījumu reģistrā, norādot saistītās izmaiņu kontroles atsauces un komunikācijas plānus.

9.4 Versiju kontrole un komunikācija

9.4.1 Jebkurai atjauninātai šīs politikas versijai:

9.4.1.1 jāietver būtiskāko izmaiņu kopsavilkums;

9.4.1.2 jābūt atkārtoti izplatītai pa oficiāliem kanāliem (piemēram, politiku portālā, LMS, iekšējos biļetenos);

9.4.1.3 jāparedz skartā personāla apliecinājums, īpaši juridiskajās, darbības, drošības un piegādātāju pārvaldības lomās.

10. Saistītās politikas un sasaiste

10.1 Šī politika darbojas kopā ar turpmāk minētajām organizācijas IDPS politikām un tās papildina:

10.1.1 P1 – Informācijas drošības politika: nosaka pamatpārvaldības principus, kas nodrošina, ka visas informācijas drošības politikas, tostarp atbilstības politikas, ir saskaņotas ar stratēģiskajām biznesa un regulatīvajām prasībām.

10.1.2 P2 – Pārvaldības lomu un atbildības politika: definē lēmumu pieņemšanas pilnvaras, tai skaitā juridiskās un atbilstības lomas, kas atbild par regulatīvo pārraudzību un pārskatatbildību.

10.1.3 P6 – Risku pārvaldības politika: atbalsta tiesisko un regulatīvo atbilstības risku izvērtēšanu, atbildību par risku un mazināšanu visā organizācijā.

10.1.4 P8 – Informācijas drošības informētības un apmācību politika: nodrošina, ka viss personāls ir informēts par atbilstības pienākumiem un saņem lomai atbilstošu apmācību.

10.1.5 P12 – Aktīvu pārvaldības politika: nostiprina tiesiskos pienākumus regulētu vai līgumisku aktīvu pārvaldībai un aizsardzībai, tostarp aktīviem, kas ietver personas datus un kritisko infrastruktūru.

10.1.6 P30 – Incidentu reaģēšanas politika: nosaka obligāto juridisko paziņošanu (piemēram, GDPR 33. pants) un eskalācijas procedūras atbilstības pārkāpuma vai regulatīva notikuma gadījumā.

10.1.7 P33 – Audita un atbilstības uzraudzības politika: nodrošina strukturētas apliecināšanas darbības, tostarp kontroles pasākumu testēšanu un pierādījumu vākšanu, kas nepieciešama iekšējai un ārējai atbilstības pārbaudei.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 4.2. punkts – Ieinteresēto pušu vajadzību un gaidu izpratne: nosaka prasību identificēt un integrēt tiesiskās un regulatīvās prasības IDPS.

11.1.2 5.1. punkts – Vadība un apņemšanās: nosaka izpildvadības pārskatatbildību par tiesiskās atbilstības izveidi un uzturēšanu organizācijā.

11.1.3 5.3. punkts – Organizatoriskās lomas, pienākumi un pilnvaras: nodrošina skaidru lomu noteikšanu juridiskajai pārraudzībai un regulatīvajai atbilstībai.

11.1.4 A pielikuma 5.36. kontrole – Atbilstība tiesiskajām, normatīvajām, reglamentējošajām un līgumiskajām prasībām: nosaka prasību identificēt un izpildīt pienākumus, kas izriet no tiesību aktiem, regulējuma un līgumiem.

11.2 ISO/IEC 27002

11.2.1 5.36. kontrole: nosaka ieviešanas vadlīnijas atbilstības pienākumu reģistra uzturēšanai, regulatīvo prasību validēšanai un strukturētai pierādījumu glabāšanai.

11.3 NIST SP 800-53 Rev.5

11.3.1 PL-1 – Drošības plānošanas politika un procedūras: nosaka, ka atbilstības prasībām jābūt iestrādātām pārvaldības struktūrās un dokumentācijā.

11.3.2 PM-1 – Informācijas drošības programmas plāns: nosaka regulatīvos kontroles pasākumus kā daļu no plašākas drošības programmas.

11.3.3 CA-7 – Nepārtraukta uzraudzība: atbalsta kontroles pasākumu efektivitātes pārraudzību attiecībā uz tiesisko un politikas prasību izpildi.

11.3.4 AU-9 – Audita informācijas aizsardzība: nodrošina, ka atbilstības audita žurnāli un ieraksti ir aizsargāti un pieejami pārbaudei.

11.4 ES GDPR (2016/679)

11.4.1 5. pants – Ar apstrādi saistītie principi: nosaka likumīgu apstrādi, pārredzamību un pārskatatbildību.

11.4.2 6. pants – Apstrādes likumība: nosaka atbilstošu tiesisko pamatu visām datu apstrādes darbībām.

11.4.3 24. pants – Pārziņa atbildība: nosaka tiešu pārskatatbildību par regulatīvās atbilstības nodrošināšanu.

11.4.4 32. pants – Apstrādes drošība: prasa ieviest atbilstošus tehniskos un organizatoriskos kontroles pasākumus.

11.4.5 33. pants – Paziņošana par pārkāpumu: nosaka, ka par personas datu aizsardzības pārkāpumiem 72 stundu laikā jāziņo attiecīgajām iestādēm.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 20.–21. pants: nosaka būtiskām un svarīgām vienībām ieviest dokumentētu pārvaldību, tiesiskās atbilstības stratēģijas un nepārtrauktu tiesisko risku pārskatīšanu.

11.6 ES DORA (2022/2554)

11.6.1 5. panta 2. punkts – IKT risku pārvaldības ietvars: nosaka tiesiskās atbilstības integrēšanu plašākās risku pārvaldības un pārraudzības funkcijās.

11.6.2 19. pants – IKT trešo pušu risks: nosaka specifiskas tiesiskās prasības līgumisko un regulatīvo pienākumu pārvaldībai saistībā ar ārējiem piegādātājiem un platformām.

11.7 COBIT 2019

11.7.1 APO12 – Riska pārvaldība: ietver tiesisko un regulatīvo atbilstību kā kritisku uzņēmuma risku pārvaldības sastāvdaļu.

11.7.2 MEA03 – Atbilstības ārējām prasībām uzraudzība: nosaka nepārtrauktu uzraudzību, izņēmumu pārvaldību un gatavību auditam visiem regulatīvo pienākumu veidiem.