					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P26					Dokumenta nosaukums: **Trešo pušu un piegādātāju 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**

Atbilstība standartiem un regulējumam

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	Operacionālā plānošana un kontrole: nosaka formālu kontroles pasākumu piemērošanu trešo pušu pakalpojumiem, kas ietekmē ISMS
ISO/IEC 27002:2022	Kontroles pasākumi 5.19–5.22	Politikas un procedūras piegādātāju attiecībām; piegādātāju riska pārvaldība; piegādātāju pakalpojumu sniegšanas pārvaldība; piegādātāju uzraudzība un pārskatīšana
NIST SP 800-53 Rev.5	SA-9, SA-10, CA-3, PS-7	Ārējo sistēmu pakalpojumi; izstrādātāja konfigurācijas pārvaldība; sistēmu starpsavienojumi; trešās puses personāla drošība
ES GDPR	28., 32., 33. pants	Apstrādātāja pienākumi, apstrādes drošība, paziņošana par personas datu aizsardzības pārkāpumu
ES NIS2	21. panta 2. punkta e–f apakšpunkts	Uz risku balstīta piegādātāju pārvaldība un drošības uzraudzība
ES DORA	28., 30. pants	IKT trešo pušu risks, kritisko IKT trešo pušu pakalpojumu sniedzēju uzraudzība
COBIT 2019	BAI05, DSS02, MEA03	Organizatorisko pārmaiņu ieviešanas pārvaldība; pakalpojumu pieprasījumu un incidentu pārvaldība; atbilstības uzraudzība, izvērtēšana un novērtēšana

1. Mērķis

1.1 Šī politika nosaka informācijas drošības prasības drošu attiecību izveidei, pārvaldībai un uzturēšanai ar trešo pušu piegādātājiem un pakalpojumu sniedzējiem.

1.2 Tā nodrošina, ka uz visiem piegādātājiem, kuriem ir piekļuve organizācijas datiem, sistēmām vai infrastruktūrai, visā pakalpojuma dzīvesciklā tiek piemēroti stingri drošības kontroles pasākumi, līgumiski aizsardzības mehānismi un nepārtraukta uzraudzība.

1.3 Politika atbalsta ISO/IEC 27001 A pielikuma kontroles pasākumus no 5.19 līdz 5.22, iekļaujot drošības prasības iepirkuma, sākotnējās piesaistes, pienācīgās pārbaudes, līgumu pārvaldības, pakalpojumu uzraudzības un sadarbības izbeigšanas procesos.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem trešo pušu piegādātājiem, darbuzņēmējiem, mākoņpakalpojumu sniedzējiem un pakalpojumu organizācijām, kas apstrādā organizācijas informācijas aktīvus vai piekļūst tiem;

2.1.2 visām iekšējām lomām, kas iesaistītas piegādātāju izvērtēšanā, sākotnējā piesaistē, līgumu slēgšanā, risku pārvaldībā, uzraudzībā vai sadarbības izbeigšanā;

2.1.3 visām attiecībām ar piegādātājiem, kas ietver piekļuvi sensitīviem datiem, integrāciju ar produkcijas pakalpojumiem vai atbalstu kritiskām darbības funkcijām.

2.2 Tā aptver gan tiešos piegādātājus, gan to apakšuzņēmējus, ja tas ir piemērojams, un ietver trešo pušu programmatūru, infrastruktūru, atbalsta un pārvaldītos pakalpojumus.

3. Mērķi

3.1 Nodrošināt, ka piegādātāju drošības riski tiek konsekventi identificēti, izvērtēti un mazināti visā sadarbības dzīvesciklā.

3.2 Iekļaut standartizētas drošības prasības visos piegādātāju līgumos, tostarp pienākumus ziņot par pārkāpumiem, audita tiesības un atbildību datu aizsardzības jomā.

3.3 Noteikt pienākumu veikt formālu pienācīgo pārbaudi un dokumentētu riska izvērtēšanu pirms sadarbības uzsākšanas ar jauniem piegādātājiem vai augsta riska pakalpojumu līgumu atjaunošanas.

3.4 Izveidot mehānismus nepārtrauktai piegādātāju atbilstības uzraudzībai, tostarp veiktspējas pārskatīšanai, auditiem un incidentu eskalācijai.

3.5 Pārvaldīt izmaiņas piegādātāju pakalpojumos un nodrošināt drošu sadarbības izbeigšanu, kā arī datu atgriešanu vai iznīcināšanu līguma izbeigšanas laikā.

3.6 Saskaņot trešo pušu drošības kontroles pasākumus ar piemērojamajām normatīvajām un līgumiskajām prasībām, tostarp GDPR, NIS2, DORA un ISO/IEC 27001 standartiem.

4. Lomas un atbildība

4.1 Informācijas drošības vadītājs (CISO)

4.1.1 Atbild par šo politiku un nodrošina tās atbilstību kopējai ISMS, risku pārvaldības un atbilstības stratēģijai.

4.1.2 Apstiprina piegādātāju klasifikācijas līmeņus, drošības pārbaužu rezultātus un augsta riska izņēmumus.

4.1.3 Piedalās būtisku piegādātāju incidentu eskalācijā un līgumsarunās par kritiskiem pakalpojumiem.

4.2 Iepirkumu un piegādātāju pārvaldības funkcija

4.2.1 Nodrošina, ka visos jaunajos un atjaunotajos piegādātāju līgumos ir iekļautas apstiprinātas drošības un datu aizsardzības klauzulas.

4.2.2 Uztur centralizētu piegādātāju reģistru un koordinē darbu ar juridisko un atbilstības funkciju par trešo pušu riska dokumentāciju.

4.2.3 Uzsāk sākotnējās piesaistes procesus un nodrošina to atbilstību pirmslīguma drošības izvērtējumiem.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika jāpārskata vismaz reizi gadā vai agrāk, ja notiek:

9.1.1 būtiskas izmaiņas iepirkumu stratēģijā vai piegādātāju ekosistēmā;

9.1.2 izmaiņas tiesiskajā vai normatīvajā regulējumā (piemēram, DORA, GDPR);

9.1.3 nozīmīgi trešo pušu incidenti, datu aizsardzības pārkāpumi vai audita neatbilstības;

9.1.4 konstatējumi no riska izvērtējumiem vai ārējām sertifikācijas institūcijām.

9.2 Pārskatīšanas process ir CISO, iepirkumu, juridiskās un risku pārvaldības funkcijas kopīga atbildība.

9.3 Visas politikas redakcijas jādokumentē ISMS dokumentu kontroles reģistrā, jānodrošina versiju kontrole un jākomunicē attiecīgajām iesaistītajām pusēm, izmantojot piegādātāju pārvaldības kanālus un darbinieku informētības programmas.

9.4 Aizstātās versijas jāarhivē vismaz trīs gadus, lai nodrošinātu izsekojamību un tiesisko atbilstību.

10. Saistītās politikas un sasaiste

10.1 P1 – Informācijas drošības politika. Nosaka vispārējo apņemšanos nodrošināt visu organizācijas darbību drošību, tostarp paļaušanos uz trešo pušu piegādātājiem un ārējiem pakalpojumu sniedzējiem.

10.2 P6 – Risku pārvaldības politika. Nosaka pieeju ar trešo pušu attiecībām saistīto risku identificēšanai, izvērtēšanai un mazināšanai, tostarp piegādātāju ekosistēmas mantotajiem vai sistēmiskiem riskiem.

10.3 P17 – Datu aizsardzības un privātuma politika. Attiecas uz visiem piegādātājiem, kas apstrādā personas datus, paredzot atbilstošus līguma noteikumus, datu pārsūtīšanas aizsardzības pasākumus un privātuma aizsardzības pēc projektēšanas principus.

10.4 P4 – Piekļuves kontroles politika. Nosaka, kā trešo pušu personāls iegūst piekļuvi organizācijas sistēmām, piemērojot uz lomām balstītas atļaujas, sesiju kontroles pasākumus un piekļuves atsaukšanas procedūras.

10.5 P22 – Žurnalēšanas un uzraudzības politika. Nosaka, ka piegādātāju piekļuve sistēmām jāuzrauga, jāreģistrē žurnālos un jāpārskata, īpaši vidēs, kur notiek privileģētas darbības vai darbības ar datiem.

10.6 P30 – Reaģēšanas uz incidentiem politika. Nosaka eskalācijas procedūras un pārkāpumu ziņošanas prasības drošības notikumiem, kuru izcelsme ir piegādātāja pusē, vai kopīgām izmeklēšanām, kas saistītas ar trešo pušu sistēmām.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001: 8.1. punkts – Operacionālā plānošana un kontrole: nosaka formālus kontroles pasākumus pār trešo pušu pakalpojumiem, kas ietekmē ISMS.

11.2 ISO/IEC 27002:2022 – Kontroles pasākumi 5.19 līdz 5.22:

11.2.1 A pielikuma kontroles pasākums 5.19 – Politikas un procedūras piegādātāju attiecībām: nosaka kontroles pasākumus piegādātāju mijiedarbības pārvaldībai.

11.2.2 A pielikuma kontroles pasākums 5.20 – Piegādātāju riska pārvaldība: koncentrējas uz piegādātāju drošības stāvokļa identificēšanu, izvērtēšanu un nepārtrauktu uzraudzību.

11.2.3 A pielikuma kontroles pasākums 5.21 – Piegādātāju pakalpojumu sniegšanas pārvaldība: nosaka prasību nodrošināt veiktspējas un drošības atbilstību līgumiskajām prasībām.

11.2.4 A pielikuma kontroles pasākums 5.22 – Piegādātāju uzraudzība un pārskatīšana: nostiprina nepieciešamību pēc nepārtrauktas trešo pušu atbilstības validācijas un atkārtotas izvērtēšanas.

11.3 NIST SP 800-53 Rev.5:

11.3.1 SA-9 – Ārējo sistēmu pakalpojumi: nosaka drošības un riska prasības sistēmām, ko ekspluatē ārējas struktūras.

11.3.2 SA-10 – Izstrādātāja konfigurācijas pārvaldība: piemērojams gadījumos, kad trešās puses piegādā programmatūru vai vides.

11.3.3 CA-3 – Sistēmu starpsavienojumi: nosaka prasību pārraudzīt un vienoties par sistēmu datu plūsmām starp struktūrām.

11.3.4 PS-7 – Trešās puses personāla drošība: nodrošina, ka darbuzņēmēji un piegādātāju personāls tiek atbilstoši pārbaudīts un uzraudzīts.

11.4 ES GDPR (2016/679):

11.4.1 28. pants – Apstrādātāja pienākumi: nosaka prasību slēgt rakstiskas vienošanās ar datu apstrādātājiem, tostarp par tehniskajiem un organizatoriskajiem pasākumiem.

11.4.2 32. pants – Apstrādes drošība: nosaka pienākumu piemērot atbilstošus aizsardzības pasākumus gan pārziņiem, gan apstrādātājiem.

11.4.3 33. pants – Paziņošana par personas datu aizsardzības pārkāpumu: nosaka prasību piegādātājiem nekavējoties ziņot pārkāpuma gadījumā.

11.5 ES NIS2 direktīva (2022/2555):

11.5.1 21. panta 2. punkta e–f apakšpunkts: nosaka prasību pēc uz risku balstītas piegādātāju pārvaldības un drošības uzraudzības, īpaši būtisko un svarīgo subjektu digitālajās piegādes ķēdēs.

11.6 ES DORA (2022/2554):

11.6.1 28. pants – IKT trešo pušu risks: nosaka pienākumus attiecībā uz riska izvērtēšanu, līgumiskiem drošības noteikumiem un izstāšanās stratēģijām finanšu pakalpojumu sniedzējiem.

11.6.2 30. pants – Kritisko IKT trešo pušu pakalpojumu sniedzēju uzraudzība: nosaka pastiprinātas uzraudzības un pārraudzības prasības galvenajiem piegādātājiem.

11.7 COBIT 2019:

11.7.1 BAI05 – Organizatorisko pārmaiņu ieviešanas pārvaldība: nodrošina, ka pārejas starp piegādātājiem tiek droši pārvaldītas.

11.7.2 DSS02 – Pakalpojumu pieprasījumu un incidentu pārvaldība: attiecas uz piegādātāju ziņotām problēmām un incidentu apstrādes integrāciju.

11.7.3 MEA03 – Atbilstības uzraudzība, izvērtēšana un novērtēšana: nostiprina piegādātāju veiktspējas mērīšanu un atbilstības uzraudzību.