					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P28S					Dokumenta nosaukums: **Ārpakalpojuma izstrādes 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 piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	5.1., 6.1. un 8. punkts	Piemērojamie kontroles pasākumi attiecībā uz informācijas drošību, piegādātājiem un izstrādi
ISO/IEC 27002:2022	5.19., 5.20. un 8.25.–8.27. kontrole	Kontroles pasākumi piegādātājiem un drošam izstrādes dzīves ciklam
NIST SP 800-53 Rev.5	SA-4, SA-9, SA-11, SA-15, SR-3	Prasības iepirkumam, piegādes ķēdei, drošai izstrādei un vienošanām ar piegādātājiem
ES GDPR	28. pants	Līgumiskās un datu aizsardzības prasības trešo personu veiktai datu apstrādei
ES NIS2	21(2)(a), (h) pants	Kontroles pasākumi piegādes ķēdes drošībai un drošai lietojumprogrammu izstrādei
ES DORA	10. pants	IKT trešo pušu risku pārvaldība, tostarp ārpakalpojuma izstrāde
COBIT 2019	BAI03, DSS05	Prasības ārējai izstrādei un IS pakalpojumu sniedzējiem

1. Mērķis

1.1 Šīs politikas mērķis ir nodrošināt, ka visa ārpakalpojuma programmatūras izstrāde neatkarīgi no tā, vai to veic ārštata speciālisti, aģentūras vai trešo pušu pakalpojumu sniedzēji, tiek īstenota droši, ar atbilstošu līgumisko kontroli un saskaņā ar piemērojamajām tiesiskajām, regulatīvajām un audita prasībām.

1.2 Tā aizsargā organizāciju pret riskiem, kas saistīti ar nedrošu kodu, neskaidru īpašumtiesību regulējumu, datu neatļautu izpaušanu un nepietiekamu piegādātāju pārvaldību, nosakot saistošus izstrādes standartus un piegādātāju pārraudzību arī tad, ja organizācijā nav atsevišķas IT struktūrvienības.

1.3 Šī politika atbalsta ISO/IEC 27001:2022 sertificēšanu, nosakot skaidras izstrādes prasības, atbildību un dokumentētus kontroles pasākumus trešo pušu veiktām izstrādes darbībām.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 visiem ārpakalpojuma izstrādātājiem, tostarp ārštata speciālistiem un izstrādes aģentūrām;

2.1.2 jebkuru izstrādes darbu, kas saistīts ar iekšējiem rīkiem, publiski pieejamām tīmekļvietnēm, programmatūras lietojumprogrammām vai biznesa procesu automatizāciju;

2.1.3 personālu, kas atbild par ārējo izstrādātāju atlasi, pārvaldību vai pārraudzību;

2.1.4 jebkuru trešās puses sistēmu integrāciju, skriptēšanu vai izstrādi, kas mijiedarbojas ar uzņēmuma datiem vai sistēmām.

2.2 Tā attiecas arī uz jebkuru personu vai platformu, kurai ir piekļuve uzņēmuma pieteikšanās datiem, datu repozitorijiem, pirmkoda repozitorijiem, testēšanas videi vai ražošanas sistēmām.

3. Mērķi

3.1 Nodrošināt, ka visa ārpakalpojuma izstrāde atbilst drošas kodēšanas principiem un ka izstrādātājiem līgumiski ir noteikts pienākums ievērot dokumentētos standartus un konfidencialitātes nosacījumus.

3.2 Noteikt īpašumtiesības uz visiem nodevumiem — kodu, resursiem, autentifikācijas datiem un dokumentāciju —, nodrošinot pilnīgu tiesību nodošanu uzņēmumam un izsekojamu nodošanas procesu projekta noslēgumā.

3.3 Novērst tipiskos izstrādes riskus, tostarp aizsargāta koda neatļautu atkārtotu izmantošanu, piegādes ķēdes uzbrukumus, izmantojot bibliotēkas, neatbalstītu ietvaru izmantošanu un nepārbaudītu administratīvo piekļuvi.

3.4 Noteikt prasību pirms sadarbības uzsākšanas noformēt dokumentāciju katram ārpakalpojuma projektam, tostarp līgumus, konfidencialitātes vienošanos un minimālās drošības prasības.

3.5 Aizsargāt klientu datus, sistēmas un iekšējos procesus, nodrošinot efektīvu izstrādes pārraudzību, testēšanu pēc piegādes un drošu piekļuves pārvaldību sistēmām.

4. Lomas un atbildība

4.1 Ģenerāldirektors (GM)

4.1.1 Apstiprina visas attiecības ar piegādātājiem un paraksta izstrādes vienošanās.

4.1.2 Nodrošina, ka visa ārpakalpojuma izstrāde atbilst šai politikai.

4.1.3 Pēc projekta pabeigšanas nodrošina piekļuves tiesību atsaukšanu uzņēmuma sistēmām.

4.1.4 Pārskata pēc piegādes saņemto dokumentāciju un rezultātus.

4.2 Projekta īpašnieks (parasti iekšējais darbinieks vai norīkots koordinators)

4.2.1 Veic ikdienas koordināciju ar ārējo izstrādātāju.

4.2.2 Pārbauda, ka funkcionālās prasības ir izpildītas un nodevumi ir notestēti.

4.2.3 Nodrošina drošu koda un autentifikācijas datu nodošanu.

4.2.4 Ziņo GM par jebkādām ar izstrādi saistītām problēmām vai incidentiem.

[... 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 ģenerāldirektoram (GM) jāpārskata vismaz reizi gadā. Pārskatīšanas mērķis ir nodrošināt, ka tā joprojām atbilst:

9.1.1.1 ISO/IEC 27001 sertifikācijas prasībām;

9.1.1.2 izmaiņām tiesiskajos pienākumos (piemēram, GDPR 28. pants, DORA 10. pants);

9.1.1.3 aktuālajai MVU līmeņa izstrādes praksei un trešo pušu riskiem.

9.2 Starpposma pārskatīšana

9.2.1 Politika jāpārskata arī tad, ja:

9.2.1.1 tiek piesaistīts jauns ārpakalpojuma izstrādes piegādātājs vai platforma;

9.2.1.2 notiek būtisks incidents, kas saistīts ar ārpakalpojuma izstrādi;

9.2.1.3 tiek veiktas būtiskas izmaiņas izmantotajos rīkos, platformās vai vidēs.

9.3 Pārskatīšanas process

9.3.1 GM ir atbildīgs par:

9.3.1.1 pārbaudi, ka līgumi, konfidencialitātes līgumi un piekļuves kontroles procesi saglabā efektivitāti;

9.3.1.2 apstiprinājumu, ka pašreizējie piegādātāji un ārštata speciālisti ievēro šo politiku;

9.3.1.3 nosacījumu pārskatīšanu, pamatojoties uz iepriekšējo projektu vai incidentu atgriezenisko saiti.

9.4 Versiju kontrole un komunikācija

9.4.1 Visām izmaiņām jābūt:

9.4.1.1 reģistrētām, norādot datumu, iemeslu un izmaiņu aprakstu;

9.4.1.2 GM apstiprinātām un iekļautām versiju vēsturē;

9.4.1.3 paziņotām visam personālam vai projektu īpašniekiem, kas sadarbojas ar ārējiem izstrādātājiem;

9.4.1.4 atkārtoti nosūtītām visiem skartajiem piegādātājiem un trešajām pusēm, ja tas nepieciešams.

10. Saistītās politikas un sasaiste

10.1 Šī politika tieši atbalsta turpmāk minēto MVU vajadzībām pielāgoto politiku ieviešanu un ir ar tām cieši saistīta:

10.1.1 P2S – Pārvaldības lomu un atbildības politika: precizē, kurš atbild par piegādātāju apstiprināšanu, piekļuves kontroli un riska pieņemšanu, izmantojot ārpakalpojuma izstrādātājus.

10.1.2 P4S – Piekļuves kontroles politika: nosaka lietotāju kontu un administratīvās piekļuves pareizu izveidi, ierobežošanu un izbeigšanu ārpakalpojuma izstrādes laikā.

10.1.3 P8S – Informācijas drošības informētības un apmācību politika: nodrošina, ka iekšējais personāls izprot, kā droši koordinēt darbu ar ārējiem izstrādātājiem, tostarp pārvaldīt autentifikācijas datus un projekta datnes.

10.1.4 P17S – Datu aizsardzības un privātuma politika: nosaka drošības un tiesiskās prasības personas datu apstrādei, ko saskaņā ar GDPR var veikt ārpakalpojuma izstrādātāji.

10.1.5 P24S – Drošas izstrādes politika: nosaka, kā iekšējā un ārējā izstrādē jāievēro drošas kodēšanas prakse un bibliotēku un ietvaru pārbaude.

10.1.6 P30S – Incidentu pārvaldības politika: piemērojama, ja ārpakalpojuma izstrāde izraisa drošības incidentus vai ievainojamības, nodrošinot koordinētu izmeklēšanu un novēršanas pasākumus.

10.2 Šīs politikas jāievieš paralēli, lai nodrošinātu, ka ārpakalpojuma izstrāde nerada nepārvaldītu risku un nepārkāpj MVU atbilstības pienākumus.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 6.1. punkts – organizācijām jāizvērtē un jāapstrādā informācijas drošības riski, kas saistīti ar piegādātājiem.

11.1.2 8.1. punkts – nosaka darbību plānošanu un kontroli, tostarp attiecībā uz trešo pušu pakalpojumiem, piemēram, ārpakalpojuma izstrādi.

11.2 ISO/IEC 27002

11.2.1 5.19. kontrole – iesaka izvērtēt piegādātāju spēju izpildīt informācijas drošības prasības.

11.2.2 5.20. kontrole – paredz regulāru trešo pušu pakalpojumu uzraudzību un periodisku pārskatīšanu.

11.2.3 8.25.–8.27. kontrole – nosaka droša izstrādes dzīves cikla praksi, kas piemērojama ārpakalpojuma izstrādei.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-4 – nosaka, ka iegādes stratēģijās jāiekļauj informācijas drošības pasākumi.

11.3.2 SA-9 – attiecas uz ārējo sistēmu izstrādi un piegādes ķēdes riskiem.

11.3.3 SA-11 – nosaka drošas izstrādes praksi, tostarp koda pārskatīšanu un ievainojamību novēršanu.

11.3.4 SA-15 – paredz automatizētu rīku izmantošanu ievainojamību noteikšanai un programmatūras kvalitātes apliecināšanai.

11.3.5 SR-3 – nosaka, ka vienošanās ar piegādātājiem ietver kiberdrošības prasības.

11.4 Eiropas Savienības Vispārīgā datu aizsardzības regula (GDPR)

11.4.1 28. pants – nosaka, ka līgumos ar trešo personu apstrādātājiem jāparedz atbilstoši datu aizsardzības drošības pasākumi; tas tieši attiecas uz izstrādātājiem, kuri apstrādā personas datus vai tiem piekļūst.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 21(2)(a), (h) pants – nosaka piegādes ķēdes drošības kontroles pasākumus un drošas programmatūras izstrādes praksi piemērošanas jomā esošiem digitālo pakalpojumu sniedzējiem, tostarp MVU, ja tas ir piemērojams.

11.6 ES Digitālās darbības noturības akts (DORA)

11.6.1 10. pants – nosaka IKT trešo pušu risku pārvaldību, tostarp izstrādes vienošanās, drošības pienākumus un riska kontroles pasākumus, kas saistīti ar trešo pušu pakalpojumu sniedzējiem.

11.7 COBIT 2019

11.7.1 BAI03 – Risinājumu identificēšanas un izveides pārvaldība – nodrošina, ka ārējā izstrāde atbilst darbības prasībām un drošības prasībām.

11.7.2 DSS05 – Drošības pakalpojumu pārvaldība – nosaka, ka ārējie drošības pakalpojumu un izstrādes sniedzēji darbojas saskaņā ar noteiktajām drošības prasībām un pārraudzību.