| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Šeit ievadiet reģistrētās juridiskās personas nosaukumu | | | | | | | |
| Dokumenta numurs:<br>P28 | | | | | Dokumenta nosaukums:<br>**Ārpakalpojuma izstrādes politika** | | | | | | | |
| Versija:<br>1.0 | | Spēkā stāšanās datums:<br>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 | Punkts 8.1 | N/A |
| ISO/IEC 27002:2022 | Kontroles pasākumi 5.19-5.22, 8 | N/A |
| NIST SP 800-53 Rev.5 | SA-4, SA-9, SA-10 | N/A |
| ES GDPR | Panti 28, 32 | N/A |
| ES NIS2 | Panti 21(2)(a), (h), 23 | N/A |
| ES DORA | Panti 28(1), (2) | N/A |
| COBIT 2019 | APO10, BAI03, DSS | N/A |

**1. Mērķis**

1.1 Šī politika nosaka obligātos kontroles pasākumus programmatūras vai sistēmu izstrādes nodošanai ārpakalpojumā ārējiem piegādātājiem, darbuzņēmējiem vai aģentūrām, nodrošinot, ka drošas prakses ir integrētas visā izstrādes dzīves ciklā.

1.2 Tās mērķis ir novērst drošības ievainojamības, datu zudumu, intelektuālā īpašuma neatļautu izpaušanu un atbilstības pārkāpumus, kas izriet no ārējās izstrādes iesaistes.

1.3 Politika nosaka piegādātāju pārvaldības, drošas kodēšanas, piekļuves pārvaldības, uzraudzības un sadarbības izbeigšanas prasības līguma darbības beigās, lai saglabātu izstrādātās programmatūras konfidencialitāti, integritāti un pieejamību (CIA).

**2. Piemērošanas joma**

**2.1 Šī politika attiecas uz visām organizācijas struktūrvienībām, kas iesaista ārējās puses programmatūras vai sistēmu izstrādei, tostarp:**

2.1.1 tīmekļlietotnēm, mobilajām lietotnēm, iegultajām sistēmām, API, skriptiem, automatizācijas darbplūsmām vai platformu moduļiem;

2.1.2 pielāgotai izstrādei iekšējām platformām, klientiem pieejamām sistēmām vai komerciāliem produktiem;

2.1.3 sadarbībai ar trešo pušu izstrādātājiem, ārštata speciālistiem, aģentūrām vai ārvalstu komandām.

2.2 Šī politika reglamentē arī jebkuru ārējo pusi, kas izstrādes laikā piekļūst pirmkodam, testēšanas vidēm vai CI/CD cauruļvadiem.

2.3 Prasības ir saistošas neatkarīgi no līguma veida, izstrādes metodoloģijas vai ārpakalpojuma sniedzēja ģeogrāfiskās atrašanās vietas.

**3. Mērķi**

3.1 Nodrošināt droša programmatūras izstrādes dzīves cikla (SDLC) prakšu piemērošanu visās ārpakalpojuma iesaistēs no plānošanas līdz validācijai pēc ieviešanas.

3.2 Nodrošināt, ka visos līgumos ar ārējiem izstrādātājiem ir iekļautas obligātas klauzulas par datu aizsardzību, drošu kodēšanu un intelektuālā īpašuma saglabāšanu.

3.3 Noteikt piekļuves kontroles, uzraudzības un audita prasības trešo pušu izstrādātājiem, kuri mijiedarbojas ar iekšējām sistēmām.

3.4 Aizsargāt organizāciju pret piegādes ķēdes apdraudējumiem, normatīvo aktu pārkāpumiem un reputācijas kaitējumu, kas saistīts ar ārēji izstrādātu programmatūru.

3.5 Uzturēt nepārtrauktu atbilstību drošības ietvariem, tostarp ISO/IEC 27001, NIST, GDPR, NIS2, DORA un COBIT 2019.

**4. Lomas un pienākumi**

**4.1 Izpildvadība**

4.1.1 Apstiprina augsta riska ārpakalpojuma izstrādes projektus un, ja pamatoti, apstiprina politikas izņēmumus.

4.1.2 Nodrošina, ka lēmumi par ārpakalpojuma izmantošanu atbilst stratēģiskajiem mērķiem un organizācijas riska apetītei.

**4.2 Galvenais informācijas drošības vadītājs (CISO)**

4.2.1 Apstiprina piegādātāju uzņemšanu no informācijas drošības perspektīvas.

4.2.2 Nosaka drošības kontroles prasības ārpakalpojuma iesaistei un pārskata incidentu ziņojumus.

[ ... 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 biežāk šādos gadījumos:**

9.1.1 tiek ieviesti jauni izstrādes ārpakalpojuma modeļi, piegādātāji vai jurisdikcijas;

9.1.2 tiek atjaunināti regulatīvie ietvari, piemēram, GDPR, NIS2 vai DORA;

9.1.3 pēc drošības incidenta, kas saistīts ar ārpakalpojuma kodu, piekļuvi vai nodevumiem;

9.1.4 kā daļa no iekšējā audita konstatējumiem vai IDPS pilnveides.

**9.2 Par politikas pārskatīšanas uzsākšanu un koordinēšanu atbild Galvenais informācijas drošības vadītājs (CISO), konsultējoties ar:**

9.2.1.1 juridisko lietu un iepirkumu funkciju (lai nodrošinātu saskaņotību ar līgumiskajām prasībām);

9.2.1.2 projektu un produktu īpašniekiem (darbības īstenojamības nodrošināšanai);

9.2.1.3 informācijas drošības funkciju (apdraudējumu un kontroles pasākumu atjauninājumiem);

9.2.1.4 Izpildvadību (galīgajam apstiprinājumam).

**9.3 Visi politikas atjauninājumi:**

9.3.1.1 jāpārvalda ar versiju kontroli un jāglabā norādītajā dokumentu repozitorijā;

9.3.1.2 jāpaziņo iesaistītajām pusēm, kas piedalās ārpakalpojuma izstrādes aktivitātēs;

9.3.1.3 jāsasaista ar jebkādiem atjauninājumiem saistītajās politikās vai procedūru dokumentācijā.

9.4 Katrai politikas versijai jāpievieno izmaiņu žurnāls, lai nodrošinātu grozījumu un apstiprinājumu izsekojamību.

**10. Saistītās politikas un sasaiste**

**10.1 Šī politika atbalsta turpmāk minētos saistītos dokumentus un tiek atbalstīta ar tiem:**

10.1.1 P1 - Informācijas drošības politika: nosaka uzņēmuma līmeņa drošības principus, kas piemērojami gan iekšējās, gan trešo pušu izstrādes kontekstā.

10.1.2 P5 - Izmaiņu pārvaldības politika: nodrošina, ka visas ar izvietošanu saistītās izmaiņas ārpakalpojuma kodu bāzēs tiek pārskatītas un apstiprinātas pirms ieviešanas.

10.1.3 P13 - Datu klasifikācijas un marķēšanas politika: nosaka, kā sensitīvi dati tiek identificēti pirms to izpaušanas izstrādes piegādātājiem vai ievietošanas repozitorijos.

10.1.4 P18 - Kriptogrāfisko kontroles pasākumu politika: nosaka, kā izstrādes un piegādes laikā jāpārvalda atslēgas, noslēpumi un sensitīvi autentifikācijas dati.

10.1.5 P24 - Drošas izstrādes politika: definē pamatprasības iekšējās un ārējās programmatūras izstrādes praksēm.

10.1.6 P30 - Incidentu reaģēšanas politika: reglamentē, kā ar ārpakalpojuma izstrādi saistīti pārkāpumi vai drošības incidenti tiek eskalēti, izmeklēti un novērsti.

10.1.7 P33 - Audita un atbilstības uzraudzības politika: nosaka prasības ārpakalpojuma izstrādes aktivitāšu pārskatīšanai auditu vai atbilstības pārbaužu laikā.

## 11. Atsauces standarti un ietvari

11.1 Šī politika ir saskaņota ar starptautiski atzītiem drošības ietvariem un regulējumu, lai nodrošinātu drošu programmatūras izstrādes nodošanu ārpakalpojumā un efektīvu piegādātāju pārvaldības praksi.

### 11.2 ISO/IEC 27001

11.2.1 Punkts 8.1 - darbības plānošana un kontrole: nosaka procesu kontroles pasākumus drošai izstrādei un trešo pušu piegādei.

### 11.3 ISO/IEC 27002:2022 - kontroles pasākumi 5.19 līdz 5.21, 8.

11.3.1 A pielikuma 5.19. kontrole - piegādātāju attiecību pārvaldība: nosaka prasību par formālām vienošanām ar drošības un atbilstības klauzulām.

11.3.2 A pielikuma 5.20. kontrole - informācijas drošības prasību iekļaušana piegādātāju līgumos: nodrošina, ka līgumos tiek iestrādāti izstrādei specifiski kontroles pasākumi.

11.3.3 A pielikuma 5.21. kontrole - piegādātāju pakalpojumu sniegšanas pārvaldība: ietver trešo pušu izstrādes nodevumu un risku uzraudzību.

11.3.4 A pielikuma 8.27. kontrole - ārpakalpojuma izstrāde: nosaka definētas drošības prasības un piekļuves kontroli pār ārēji izstrādātu programmatūru.

11.3.5 Šie kontroles pasākumi nosaka strukturētas prasības ārpakalpojuma izstrādātāju atlasei, līgumu slēgšanai un pārraudzībai, tostarp drošas izstrādes praksei, koda apstrādei un snieguma pārbaudei.

### 11.4 NIST SP 800-53 Rev.5

11.4.1 SA-4 - iegādes process: nosaka, ka drošas izstrādes prasības jādefinē iegādes brīdī.

11.4.2 SA-9 - ārējo sistēmu pakalpojumi: reglamentē, kā trešo pušu izstrādātāji droši mijiedarbojas ar iekšējiem pakalpojumiem.

11.4.3 SA-10 - izstrādātāja konfigurācijas pārvaldība: atbilst versiju kontroles, koda piekļuves un izmaiņu uzskaites pienākumiem ārējām komandām.

### 11.5 ES GDPR (2016/679)

11.5.1 28. pants - apstrādātāja pienākumi: nosaka, ka līgumos ar trešo pušu izstrādātājiem jāparedz drošības, kontroles un audita prasības personas datu apstrādei.

11.5.2 32. pants - apstrādes drošība: nosaka atbilstošus drošības pasākumus (piemēram, šifrēšanu, piekļuves kontroli), izstrādājot sistēmas, kas apstrādā personas datus.

### 11.6 ES NIS2 direktīva (2022/2555)

11.6.1 Panti 21(2)(a), (h), 23: nosaka, ka drošas izstrādes prakse jāpiemēro visās trešo pušu iesaistēs un digitālajās piegādes ķēdēs, nodrošinot pārraudzību un tehnisko pārbaudi.

### 11.7 ES DORA (2022/2554)

11.7.1 Panti 28(1), (2): nosaka, ka finanšu iestādēm jāpārvalda IKT trešo pušu risks, izmantojot līgumiskos kontroles pasākumus un drošas izstrādes pārraudzību, īpaši kritiskas ārpakalpojuma izstrādes gadījumā.

### 11.8 COBIT 2019

11.8.1 APO10 - piegādātāju pārvaldība: nosaka strukturētas prasības piegādātāju izvērtēšanai, līgumiem un snieguma uzraudzībai.

11.8.2 BAI03 - risinājumu izstrādes pārvaldība: tieši atbilst droša SDLC procesiem, koda pārskatīšanai un izstrādes validācijai.

11.8.3 DSS05 - drošības pakalpojumu pārvaldība: atbilst ārēji vai trešo pušu izstrādātu sistēmu uzraudzībai un aizsardzībai.