					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P24S					Dokumenta nosaukums: **Drošas 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**

Saskaņotība ar piemērojamajiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	Attiecināmi drošības kontroles pasākumi darbības praksēs, tostarp drošā izstrāde
ISO/IEC 27002:2022	8.25–8.27. kontroles pasākumi	Aptver drošas izstrādes dzīves ciklu, testēšanu un trešo pušu izstrādātāju drošības pienākumus
NIST SP 800-53 Rev.5	SA-3–SA-15, SI-10	Aptver drošu SDLC, piekļuves kontroli un ievainojamību apstrādi izstrādes procesā
ES GDPR	25. pants	Nosaka datu aizsardzību pēc projektēšanas un pēc noklusējuma programmatūras izstrādē
ES NIS2	21. panta 2. punkta a), e), h) apakšpunkts	Nosaka pienākumu ieviest drošas izstrādes politikas, pārraudzīt atvērtā pirmkoda izmantošanu un dokumentēt risku mazināšanas pasākumus
ES DORA	6. panta 7. punkts, 9. panta 1. punkta c) apakšpunkts, 10. panta 2. punkta c) apakšpunkts	Dzīves cikla drošība kritiskām IKT sistēmām finanšu sektorā
COBIT 2019	BAI	Ietvars strukturētai, izsekojamai un noturīgai drošas izstrādes pārvaldībai

1. Mērķis

1.1 Šī politika nodrošina, ka visa programmatūra, skripti un tīmekļa risinājumi, ko organizācija vai tās ārējie partneri izstrādā vai modificē, tiek izstrādāti droši, samazinot ievainojamību, neatļautas piekļuves datiem un darbības traucējumu risku.

1.2 Tā nosaka obligātās drošas izstrādes prasības un drošas kodēšanas praksi, kas jāievēro visiem iekšējiem izstrādātājiem, līgumslēdzējiem un piegādātājiem neatkarīgi no projekta apjoma vai sarežģītības.

1.3 Šīs politikas mērķis ir aizsargāt klientu datus, novērst drošības incidentus un nodrošināt, ka organizācijas vajadzībām vai tās uzdevumā izstrādāta vai pielāgota programmatūra spēj izturēt drošības auditus, atbilst normatīvajām prasībām (piemēram, GDPR, NIS2, DORA) un atbalsta ISO/IEC 27001 sertifikāciju.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām personām un vienībām, kas organizācijas vārdā piedalās šādu risinājumu izstrādē, pielāgošanā, ieviešanā vai pārvaldībā:

2.1.1 tīmekļvietnes, lietotnes vai automatizācijas rīki;

2.1.2 iekšēji izstrādāti skripti vai programmatūra;

2.1.3 pirmkods, ko izstrādājuši trešo pušu izstrādātāji vai ārštata speciālisti;

2.1.4 spraudņi, bibliotēkas un programmatūras komponenti, kas integrēti ražošanas sistēmās.

2.2 Tā attiecas uz visām vidēm, ko izmanto izstrādes darbībās, tostarp:

2.2.1 izstrādes un testēšanas vidēm;

2.2.2 sagatavošanas un pirmsražošanas vidēm;

2.2.3 ražošanas sistēmām, kurās tiek darbināts individuāli izstrādāts pirmkods.

2.3 Politika regulē arī datu apstrādi izstrādes un ieviešanas laikā, jo īpaši jebkādu ražošanas datu izmantošanu neprodukcijas sistēmās.

3. Mērķi

3.1 Novērst drošības trūkumu vai ievainojamību ieviešanu individuāli izstrādātā vai trešo pušu izstrādātā programmatūrā.

3.2 Nodrošināt, ka drošas kodēšanas prakse un ievainojamību novēršana ir integrēta katrā programmatūras izstrādes dzīves cikla posmā.

3.3 Samazināt riskus, kas saistīti ar atvērtā pirmkoda vai trešo pušu komponentu izmantošanu, nosakot pienākumu veikt pienācīgu pārbaudi un uzturēt uzskaiti.

3.4 Noteikt obligātu formālu pirmkoda pārskatīšanu un lietotņu drošības testēšanu pirms nodošanas ekspluatācijā.

3.5 Kontrolēt piekļuvi izstrādes vidēm un nodrošināt to nošķiršanu no aktīvajām ražošanas sistēmām.

3.6 Izpildīt obligātās prasības saskaņā ar starptautiskajiem standartiem un regulējumu (piemēram, ISO/IEC 27001, GDPR, DORA, NIS2).

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 apstiprina šo politiku un ir tās īpašnieks;

4.1.2 nodrošina, ka visa programmatūras izstrāde (iekšēja vai ārpakalpojumā) atbilst šai politikai;

4.1.3 pārskata un paraksta izstrādes vai pakalpojumu līgumus, kuros iekļautas drošas izstrādes klauzulas;

4.1.4 pārbauda piegādātāju atbilstību, veicot regulāras pārbaudes vai pieprasot drošības apliecinājumus.

4.2 Iekšējais izstrādātājs vai lietotnes īpašnieks

4.2.1 ievēro drošas kodēšanas un ieviešanas praksi;

4.2.2 piemēro drošas izstrādes kontrolsarakstu katram projektam;

4.2.3 pārbauda izmantoto atvērtā pirmkoda vai trešo pušu komponentu drošību;

4.2.4 nekavējoties ziņo GM par jebkuru atklātu ievainojamību.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Ģenerāldirektoram šī politika jāpārskata vismaz reizi gadā, lai:

9.1.1 pārbaudītu turpmāku atbilstību ISO/IEC 27001, GDPR, NIS2 un DORA;

9.1.2 atspoguļotu aktualizētos apdraudējumus vai izmaiņas drošas izstrādes labākajā praksē;

9.1.3 nodrošinātu savietojamību ar jauniem rīkiem, platformām vai sadarbību ar piegādātājiem.

9.2 Starpposma pārskatīšana jāierosina šādos gadījumos:

9.2.1 jebkurš ziņots programmatūras drošības incidents;

9.2.2 jauna izstrādes ietvara vai mitināšanas platformas ieviešana;

9.2.3 izmaiņas trešo pušu izstrādes partneros;

9.2.4 regulējuma atjauninājumi, kas ietekmē programmatūras vai drošības pienākumus.

9.3 Visi šīs politikas grozījumi:

9.3.1 jādokumentē, norādot datumu, izmaiņu kopsavilkumu un GM apstiprinājumu;

9.3.2 skaidri jāpaziņo visam iekšējam un ārējam izstrādes personālam;

9.3.3 jāglabā kā daļa no organizācijas politiku versiju kontroles un izmaiņu vēstures.

9.4 Atjauninātajām versijām jābūt viegli pieejamām — iekšējās platformās, drukātā dokumentācijā vai piegādātājiem pieejamos mākoņpakalpojumos.

10. Saistītās politikas un sasaiste

10.1 Šī politika atbalsta vairāku citu SME politiku sekmīgu ieviešanu un ir ar tām saistīta:

10.1.1 P2S – Pārvaldības lomu un atbildības politika: nosaka atbildību par izstrādes drošības kontroles pasākumu piešķiršanu un pārbaudi projektu un piegādātāju ietvaros.

10.1.2 P4S – Piekļuves kontroles politika: nosaka pamatnoteikumus piekļuves ierobežošanai izstrādes vidēm un pirmkoda repozitorijiem, tostarp pienākumu nodalīšanu.

10.1.3 P8S – Informācijas drošības informētības un apmācības politika: nodrošina, ka iekšējie izstrādātāji un līgumslēdzēji izprot drošas kodēšanas praksi un ar to saistītos drošības pienākumus.

10.1.4 P17S – Datu aizsardzības un privātuma politika: precizē, kā personas dati jāapstrādā izstrādes, testēšanas un žurnālfiksēšanas procesos, lai nodrošinātu atbilstību GDPR.

10.1.5 P30S – Incidentu pārvaldības politika: nosaka, kā jāziņo par ar izstrādi saistītiem drošības incidentiem, kā tie jāizvērtē un kā jānovērš to sekas, tostarp gadījumos, kas saistīti ar pirmkoda radītu pakļautību riskam.

10.2 Šīs politikas kopumā nodrošina, ka droša izstrāde ir īstenojama un pārbaudāma arī mazā vai netehniskā organizācijā.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8. punkts – nosaka pienākumu ieviest darbības kontroles pasākumus, tostarp drošu izstrādi, atbilstoši biznesa mērķiem un riska stāvoklim.

11.2 ISO/IEC 27002

11.2.1 8.25. kontrole – iesaka integrēt drošību visā programmatūras dzīves ciklā, tostarp pirmkoda kontrolē, versiju pārvaldībā un izstrādātāju piekļuvē.

11.2.2 8.26. kontrole – nosaka lietotņu testēšanas metodes un drošības funkcionalitātes pārbaudi pirms nodošanas ražošanas vidē.

11.2.3 8.27. kontrole – nosaka, ka trešo pušu izstrādātājiem jāievēro tie paši izstrādes standarti un ka viņu drošības pienākumi jādefinē skaidri.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 līdz SA-15 – nosaka drošas izstrādes procesus, tostarp izstrādātāju piekļuves kontroli, testēšanu, apdraudējumu modelēšanu un dokumentēšanu.

11.3.2 SI-10 – nosaka pienākumu izstrādātājiem identificēt un mazināt izplatītus programmatūras trūkumus un, kur piemērojams, izmantot automatizētus rīkus.

11.4 ES GDPR (2016/679)

11.4.1 25. pants – “datu aizsardzība pēc projektēšanas un pēc noklusējuma” nosaka pienākumu programmatūras projektēšanā un izstrādē integrēt drošības un privātuma aizsardzības pasākumus, jo īpaši gadījumos, kad tiek apstrādāti personas dati.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 21. panta 2. punkta a), e) un h) apakšpunkts – nosaka pienākumu ieviest drošas izstrādes politikas, pārraudzīt atvērtā pirmkoda izmantošanu un dokumentēt ar lietotnēm saistīto risku mazināšanu būtiskajās un svarīgajās vienībās.

11.6 ES DORA (2022/2554)

11.6.1 6. panta 7. punkts, 9. panta 1. punkta c) apakšpunkts un 10. panta 2. punkta c) apakšpunkts – nosaka izstrādes dzīves cikla drošības pienākumus finanšu sektora subjektiem, tostarp SME, jo īpaši attiecībā uz kritiskām IKT sistēmām.

11.7 COBIT 2019

11.7.1 BAI03 – “Risinājumu identificēšanas un izveides pārvaldība” atbalsta strukturētu izstrādes kontroles pasākumu ieviešanu, uzsverot drošību, izsekojamību un noturību, pielāgojot tos SME ierobežojumiem.