					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P24					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**

1. Mērķis

1.1 Šī politika nosaka obligātās drošības prasības programmatūras un sistēmu izstrādes darbībām organizācijā, tostarp iekšējiem projektiem, ārpakalpojuma izstrādei un trešo pušu koda integrācijai.

1.2 Tās mērķis ir nodrošināt, ka drošība tiek integrēta visā programmatūras izstrādes dzīves ciklā (SDLC) un ka ievainojamības tiek identificētas, mazinātas un novērstas pirms nodošanas ražošanas vidē.

1.3 Šī politika atbalsta ISO/IEC 27001:2022 8. punkta un A pielikuma 8.25–8.28 kontroles pasākumu ieviešanu, standartizējot drošas izstrādes pārvaldību, koda validācijas praksi un trešo pušu izstrādes uzraudzību.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 iekšēji vai ārēji izstrādātu programmatūru, lietotnēm, skriptiem, integrācijām un automatizācijas rīkiem

2.1.2 izstrādes komandām, produktu īpašniekiem, DevOps speciālistiem, kvalitātes nodrošināšanas speciālistiem, arhitektiem, projektu vadītājiem un līgumslēdzējiem

2.1.3 SDLC vidēm, tostarp izstrādes, testēšanas, sagatavošanas un pirmsražošanas sistēmām

2.1.4 atvērtā pirmkoda un trešo pušu komponentēm, kas integrētas iekšējās lietotnēs

2.1.5 programmatūru, kas izvietota lokāli, privātajā mākonī, hibrīdvidē vai publiskajā mākonī

2.2 Visi lietotāji un struktūrvienības, kas organizācijas ietvaros piedalās sistēmu izstrādē, testēšanā vai izvietošanā, ir pakļauti šai politikai, tostarp pārvaldīto pakalpojumu sniedzēji (MSP) un platformu piegādātāji.

3. Mērķi

3.1 Integrēt drošības kontroles pasākumus visās programmatūras izstrādes fāzēs no projektēšanas līdz izvietošanai, nodrošinot proaktīvu un nepārtrauktu riska mazināšanu.

3.2 Novērst izmantojamu ievainojamību ieviešanu, piemēram, injekciju ievainojamības, nedrošu autentifikāciju un pakļautību zināmām trešo pušu vājajām vietām.

3.3 Izveidot un piemērot drošas programmēšanas praksi, kas ir saskaņota ar OWASP, SANS CWE un konkrētiem ietvariem piemērojamām vadlīnijām.

3.4 Nodrošināt, ka visam kodam pirms izvietošanas tiek veikta līdzinieku pārskatīšana, automatizēta analīze un drošības validācija.

3.5 Pārvaldīt izstrādes riskus, kas izriet no ārpakalpojuma darbībām, trešo pušu koda iekļaušanas un atvērtā pirmkoda programmatūras atkārtotas izmantošanas.

3.6 Aizsargāt izstrādes, testēšanas un sagatavošanas vides no nesankcionētas piekļuves un nepieļaut ražošanas datu izmantošanu bez apstiprinātas maskēšanas vai anonimizācijas.

3.7 Veicināt drošības izpratni izstrādātāju, produktu vadītāju un kvalitātes nodrošināšanas speciālistu vidū, izmantojot lomām balstītus apmācību moduļus un nepārtrauktus atjauninājumus par jauniem riskiem.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO)

4.1.1 Ir šīs politikas īpašnieks un nodrošina drošas izstrādes prasību ieviešanu visā organizācijā.

4.1.2 Apstiprina drošas programmēšanas standartus un trešo pušu izstrādes līgumus.

4.1.3 Validē riska apstrādes lēmumus par neatrisinātām vai atliktām ievainojamībām.

4.2 Lietotņu drošības vadītājs / DevSecOps vadītājs

4.2.1 Izstrādā, uztur un popularizē drošas programmēšanas vadlīnijas.

4.2.2 Integrē statisko un dinamisko drošības testēšanu CI/CD cauruļvados.

4.2.3 Veic koda drošības pārskatīšanu un nosaka obligātos trūkumu novēršanas pasākumus.

[... 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 reizi gadā vai biežāk, reaģējot uz:

9.1.1 būtiskām izmaiņām izstrādes metodoloģijās vai DevOps rīkos

9.1.2 būtiskiem drošības incidentiem, kas radušies lietotņu ievainojamību dēļ

9.1.3 izmaiņām normatīvajās prasībās attiecībā uz drošu programmatūru (piemēram, VDAR, DORA)

9.1.4 jauniem nozares standartiem vai draudu izlūkošanas informāciju (piemēram, OWASP Top 10, SLSA, MITRE CWE)

9.2 Politikas pārskatīšanu vada lietotņu drošības vadītājs sadarbībā ar CISO, programmatūras arhitektiem, kvalitātes nodrošināšanas vadību un juridisko funkciju (ja tas attiecas uz trešo pušu koda ietekmi).

9.3 Visi grozījumi jāreģistrē ISMS dokumentu kontroles reģistrā, jāpakļauj versiju kontrolei un jāpaziņo ietekmētajām komandām ar laidiena piezīmju vai obligāto apmācību starpniecību.

9.4 Iepriekšējās versijas jāsaglabā arhīva repozitorijā juridiskajai un audita izsekojamībai.

10. Saistītās politikas un sasaiste

10.1 P1 – Informācijas drošības politika. Nosaka stratēģisko mandātu drošības integrēšanai visās informācijas sistēmās, kur droša izstrāde ir viens no pamatkontroles pasākumiem.

10.2 P4 – Piekļuves kontroles politika. Definē kontroles pasākumus piekļuves ierobežošanai izstrādes vidēm, repozitorijiem, būvēšanas rīkiem un CI/CD cauruļvadiem.

10.3 P5 – Izmaiņu pārvaldības politika. Nodrošina, ka koda izmaiņām, laidieniem un izvietošanai tiek piemērota atbilstoša apstiprināšana, izmaiņu atsaukšanas plānošana un pārbaude pēc izvietošanas.

10.4 P12 – Aktīvu pārvaldības politika. Atbalsta izstrādes vidi, pirmkoda repozitoriju un būvēšanas sistēmu uzskaiti kā pārvaldītus aktīvus, uz kuriem attiecas klasificēšana un aizsardzība.

10.5 P22 – Žurnālfiksēšanas un uzraudzības politika. Attiecas uz izstrādes cauruļvadiem, nodrošinot, ka būvēšanas procesi, koda virzīšana un izvietošanas notikumi tiek reģistrēti žurnālos, uzraudzīti un analizēti drošības anomāliju noteikšanai.

10.6 P30 – Incidentu reaģēšanas politika. Nodrošina ietvaru drošības trūkumu analīzei un reaģēšanai uz tiem pēc izvietošanas vai lietotņu drošības testēšanas laikā.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8. punkts – darbības plānošana un kontrole: prasa drošas izstrādes procesu un kontroles pasākumu integrāciju darbībās.

11.2 ISO/IEC 27002:2022 – 8.25–8.28 kontroles pasākumi

11.2.1 A pielikuma 8.25. kontroles pasākums – drošs izstrādes dzīves cikls: nosaka formālu drošības integrēšanu programmatūras projektēšanā un izstrādē.

11.2.2 A pielikuma 8.26. kontroles pasākums – lietotņu drošības prasības: prasa noteikt drošas programmēšanas un drošības pieņemšanas kritērijus.

11.2.3 A pielikuma 8.27. kontroles pasākums – droša sistēmu arhitektūra un inženierijas principi: prasa piemērot drošības projektēšanas principus un mazināt zināmās vājās vietas.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-3 līdz SA-15: nosaka strukturētu lietotņu drošības izstrādes praksi, tostarp prasības projektēšanai, koda integritātei un testēšanai.

11.3.2 SI-10 – informācijas ievades validācija: attiecas uz drošas programmēšanas aizsardzības pasākumiem.

11.3.3 SR-3 – piegādes ķēdes aizsardzība: prasa pārbaudīt trešo pušu programmatūru, komponentes un izstrādes pakalpojumu sniedzējus.

11.4 ES VDAR (2016/679)

11.4.1 25. pants – datu aizsardzība pēc projektēšanas un pēc noklusējuma: nosaka pienākumu integrēt drošību un privātumu sistēmu izstrādē.

11.4.2 32. pants – apstrādes drošība: atbalsta tehniskos pasākumus, piemēram, ievaddatu validāciju, piekļuves kontroles pasākumus un drošu izvietošanu.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 21. panta 2. punkta e) un f) apakšpunkts: prasa programmatūras izstrādes praksi, kas ietver ievainojamību pārvaldību, koda drošību un ziņošanu par incidentiem.

11.6 ES DORA (2022/2554)

11.6.1 9. pants – IKT risku pārvaldība: prasa drošas izstrādes praksi finanšu subjektiem, tostarp programmatūras kvalitātes kontroles pasākumus un defektu novēršanu.

11.6.2 10. pants – darbības nepārtrauktība un testēšana: veicina stingru IKT sistēmu, tostarp lietotņu, testēšanu un validēšanu.

11.7 COBIT 2019

11.7.1 BAI03 – risinājumu identificēšanas un izveides pārvaldība: reglamentē projektēšanu, izstrādi un drošības integrāciju jaunos risinājumos.

11.7.2 BAI07 – izmaiņu pieņemšanas un pārejas pārvaldība: nodrošina drošu izvietošanu un izvērtēšanu pēc izvietošanas.

11.7.3 DSS05 – drošības pakalpojumu pārvaldība: piemēro drošības validāciju programmatūras un pakalpojumu nodrošināšanai.