					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P25					Dokumenta nosaukums: **Lietojumprogrammu drošības prasību 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**

Juridiskais paziņojums (autortiesības un lietošanas ierobežojumi)
(C) 2025 Clarysec LLC. All rights reserved.

Šis dokuments ir Clarysec LLC intelektuālais īpašums. Nevienu šī dokumenta daļu nedrīkst kopēt, atkārtoti izmantot, izplatīt vai grozīt komerciāliem vai ieviešanas nolūkiem bez iepriekšējas skaidras rakstiskas atļaujas.
Neautorizēta lietošana ir stingri aizliegta un var izraisīt tiesvedību.
Par licencēšanu sazinieties: info@clarysec.com

Saskaņotība ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	—
ISO/IEC 27002:2022	Kontroles pasākumi 8.25–8.26	—
NIST SP 800-53 Rev.5	SA-11, SA-15, SI-10	—
ES VDAR	25., 32. pants	—
ES NIS2	21(2)(f), 23. pants	—
ES DORA	9., 11. pants	—
COBIT 2019	BAI03, BAI09, DSS05	—

1. Mērķis

1.1 Šī politika nosaka obligātās lietojumprogrammu slāņa drošības prasības programmatūrai, ko organizācija izstrādā, iegādājas, integrē vai ievieš. Tā nodrošina, ka visas lietojumprogrammas tiek projektētas, ieviestas un uzturētas atbilstoši drošas izstrādes principiem, atbilstības prasībām un organizācijas riska apetītei.

1.2 Politika nosaka drošības prasību integrēšanu visā lietojumprogrammas dzīves ciklā, aptverot lietotāju autentifikāciju, datu apstrādes praksi, saskarņu aizsardzību un drošu mijiedarbību ar API un pakalpojumiem.

1.3 Ieviešot šo politiku, organizācijas mērķis ir novērst programmatūras ievainojamību rašanos, aizsargāt sensitīvus datus un nodrošināt izsekojamību un noturību pret ekspluatācijas paņēmieniem un ļaunprātīgu izmantošanu.

2. Piemērošanas joma

2.1 Šī politika attiecas uz:

2.1.1 organizācijā iekšēji izstrādātām vai ārēji iegādātām lietojumprogrammām, tostarp SaaS risinājumiem un pēc pasūtījuma izstrādātiem rīkiem;

2.1.2 lietojumprogrammām, kas atbalsta darbībai kritiskus procesus, klientu piekļuvi vai reglamentētu datu apstrādi;

2.1.3 izstrādes, DevOps, kvalitātes nodrošināšanas, produktu un drošības komandām;

2.1.4 trešo pušu izstrādātājiem, programmatūras piegādātājiem un integrācijas partneriem, kuriem ir piekļuve organizācijas lietojumprogrammām vai API.

2.2 Tā ir piemērojama visās vidēs: izstrādes, testēšanas, pirmražošanas, ražošanas un katastrofu atkopšanas vidē neatkarīgi no tā, vai tās ir izvietotas uz vietas, privātos datu centros vai publiskajā mākoņvidē.

3. Mērķi

3.1 Noteikt pamatlīmeņa funkcionālās un nefunkcionālās drošības prasības, kas jāizpilda visām lietojumprogrammām neatkarīgi no izstrādes metodes vai tehnoloģiju steka.

3.2 Nodrošināt lietojumprogrammu slāņa aizsardzības pasākumu integrēšanu, tostarp ievades validāciju, izvades kodēšanu, kļūdu apstrādi un sesiju aizsardzību.

3.3 Noteikt drošu autentifikācijas, autorizācijas un piekļuves kontroles mehānismu ieviešanu atbilstoši organizācijas identitāšu un piekļuves pārvaldības (IAM) politikām.

3.4 Noteikt obligātu drošu mijiedarbību ar API, tīmekļa saskarnēm un trešo pušu komponentēm, izmantojot apstiprinātus protokolus un drošības kontroles pasākumus.

3.5 Nodrošināt ievainojamību agrīnu atklāšanu un novēršanu, izmantojot statisko un dinamisko analīzi, koda pārskatīšanu un apdraudējumu modelēšanu.

3.6 Aizsargāt sensitīvus datus atbilstoši normatīvajām prasībām, piemērojot šifrēšanu, klasificēšanu un datu glabāšanas noteikumus.

3.7 Nodrošināt nepārtrauktu lietojumprogrammu drošības stāvokļa validāciju pēc ieviešanas, veicot testēšanu, uzraudzību un nodrošinot gatavību auditam.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO)

4.1.1 Ir šīs politikas īpašnieks un nodrošina tās atbilstību organizācijas informācijas drošības stratēģijai un riska profilam.

4.1.2 Apstiprina lietojumprogrammu drošības prasības un nodrošina obligāto kontroles pasākumu piemērošanu izstrādes un iepirkumu funkcijās.

4.2 Lietojumprogrammu drošības vadītājs / DevSecOps vadītājs

4.2.1 Nosaka pamatlīmeņa drošības kontroles pasākumus un testēšanas metodoloģijas lietojumprogrammu komponentēm.

4.2.2 Pārrauga tādu rīku kā SAST, DAST, IAST un SCA drošu integrāciju programmatūras piegādes konveijerā.

4.2.3 Uztur Lietojumprogrammu drošības prasību kontrolsarakstu un validācijas kritērijus.

[... 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 kritisku ievainojamību atklāšanu, kas ietekmē plaši izmantotus ietvarus vai atkarības;

9.1.2 izmaiņām lietojumprogrammu drošības atbilstības prasībās, piemēram, NIS2 vai DORA;

9.1.3 būtiskām izmaiņām organizācijas programmatūras izstrādes praksē, rīkos vai mākoņarhitektūrā;

9.1.4 iekšējā audita vai ārējo ielaušanās testu konstatējumiem.

9.2 Pārskatīšanu vada Lietojumprogrammu drošības vadītājs sadarbībā ar CISO, DevOps inženierijas, Juridiskās funkcijas, Iepirkumu un kvalitātes nodrošināšanas vadītājiem.

9.3 Visi grozījumi jāpakļauj versiju kontrolei IDPS dokumentu kontroles reģistrā un jāizplata visām skartajām izstrādes un produktu komandām.

9.4 Aizstātās versijas jāarhivē vismaz trīs gadus, lai nodrošinātu izsekojamību, auditējamību un atbalstu pārkāpumu izmeklēšanā.

10. Saistītās politikas un sasaiste

10.1 P1 – Informācijas drošības politika. Tā nosaka pamatu sistēmu un datu aizsardzībai, kuras ietvaros jāīsteno lietojumprogrammu līmeņa kontroles pasākumi, lai novērstu nesankcionētu piekļuvi, datu noplūdes un ekspluatācijas paņēmienus.

10.2 P4 – Piekļuves kontroles politika. Tā nosaka identitāšu un sesiju pārvaldības standartus, kas jāpiemēro visām lietojumprogrammām, tostarp stingru autentifikāciju, minimāli nepieciešamās tiesības un piekļuves tiesību pārskatīšanas prasības.

10.3 P5 – Izmaiņu pārvaldības politika. Tā regulē lietojumprogrammu koda un konfigurāciju virzīšanu uz ražošanas vidēm, nodrošinot, ka nesankcionētas vai netestētas izmaiņas tiek bloķētas.

10.4 P17 – Datu aizsardzības un privātuma politika. Tā nosaka, ka lietojumprogrammām jāīsteno datu aizsardzība pēc projektēšanas un jānodrošina personas datu un sensitīvu datu likumīga apstrāde, šifrēšana un glabāšana visās vidēs.

10.5 P24 – Drošas izstrādes politika. Tā sniedz plašāku ietvaru drošības integrēšanai SDLC, savukārt šī politika nosaka konkrētās prasības un tehniskos kontroles pasākumus, kas jāievieš lietojumprogrammu slānī.

10.6 P30 – Incidentu reaģēšanas politika. Tā nosaka strukturētu lietojumprogrammu drošības incidentu apstrādi, tostarp pēc ieviešanas vai ielaušanās testēšanas laikā identificētas ievainojamības, un paredz eskalācijas, ierobežošanas un atjaunošanas procedūras.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001:2022

11.1.1 8.1. punkts – darbības plānošana un kontrole: nosaka, ka lietojumprogrammu drošība jāintegrē procesos un sistēmās, lai nodrošinātu konfidencialitāti, integritāti un pieejamību.

11.2 ISO/IEC 27002:2022

11.2.1 Kontroles pasākumi 8.25–8.26: nosaka prasības lietojumprogrammu slāņa drošībai, tostarp drošas kodēšanas praksei, apdraudējumu modelēšanai, arhitektūras kontroles pasākumiem un trešo pušu programmatūras validācijai.

11.2.2 A pielikuma 8.25. kontrole – drošs izstrādes dzīves cikls: nosaka drošības integrēšanu visā lietojumprogrammas dzīves ciklā.

11.2.3 A pielikuma 8.26. kontrole – lietojumprogrammu drošības prasības: nosaka tehnisko kontroles pasākumu definēšanu un piemērošanu, lai aizsargātu lietojumprogrammas pret nepareizu lietošanu un kompromitēšanu.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – izstrādātāju drošības testēšana un izvērtēšana: nosaka statisko, dinamisko un ielaušanās testēšanu izstrādes laikā.

11.3.2 SA-15 – izstrādes process, standarti un rīki: nosaka formālus standartus drošai lietojumprogrammu izstrādei.

11.3.3 SI-10 – informācijas ievades validācija: nosaka kontroles mehānismus injekciju un parsēšanas uzbrukumu novēršanai.

11.4 ES VDAR (2016/679)

11.4.1 25. pants – datu aizsardzība pēc projektēšanas un pēc noklusējuma: nosaka datu aizsardzības un privātuma integrēšanu lietojumprogrammu loģikā un darbplūsmās.

11.4.2 32. pants – apstrādes drošība: nosaka atbilstošus tehniskos pasākumus, piemēram, ievades validāciju, šifrēšanu un drošus piekļuves kontroles pasākumus.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 21(2)(f) pants: nosaka ievainojamību apstrādi un drošas lietojumprogrammu dzīves cikla prakses būtiskām un svarīgām vienībām.

11.5.2 23. pants – ziņošana par drošības incidentiem: nosaka nepieciešamību pēc lietojumprogrammu slāņa žurnālfiksēšanas un uzraudzības iespējām būtisku incidentu atklāšanai un ziņošanai.

11.6 ES DORA (2022/2554)

11.6.1 9. pants – IKT risku pārvaldība: uzliek finanšu iestādēm pienākumu nodrošināt, ka lietojumprogrammas ir drošas, testētas un noturīgas pret kiberdraudiem.

11.6.2 11. pants – IKT rīku testēšana: veicina periodisku kritisku lietojumprogrammu un pakalpojumu ielaušanās testēšanu un red team vingrinājumus.

11.7 COBIT 2019

11.7.1 BAI03 – risinājumu identificēšanas un izveides pārvaldība: nosaka projektēšanas un kontroles prasības lietojumprogrammu izstrādes laikā.

11.7.2 BAI09 – lietojumprogrammu pārvaldība: uzsver drošu aktīvu lietojumprogrammu uzturēšanu, uzraudzību un pilnveidošanu.

11.7.3 DSS05 – drošības pakalpojumu pārvaldība: sasaista lietojumprogrammu aizsardzību ar plašākām organizācijas drošības operācijām un kontroles pasākumiem.