					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P25S					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**

Saskaņots ar piemērojamiem standartiem un regulējumu

Standarts/regulējums	Punkts/pants	Piezīme
ISO/IEC 27001:2022	8. punkts	Darbības kontroles pasākumi, tostarp lietojumprogrammu drošība
ISO/IEC 27002:2022	Kontroles pasākumi 8.25–8.26	Droša projektēšana, izstrāde, testēšana un koda pārskatīšana
NIST SP 800-53 Rev.5	SA-11, SI-10	Izstrādātāju un lietojumprogrammu testēšana, koda analīze, trūkumu novēršana
ES VDAR	25. pants	Datu aizsardzība pēc noklusējuma un integrēti pēc projektēšanas
ES NIS2	21. panta 2. punkta a) un e) apakšpunkts	Tehniskie pasākumi lietojumprogrammu aizsardzībai un risku identificēšanai
ES DORA	9. panta 2. punkta c) apakšpunkts, 10. panta 2. punkta c) apakšpunkts	Lietojumprogrammu drošība digitālās darbības noturības nodrošināšanai
COBIT 2019	BAI03	Drošas programmatūras izstrādes un iegādes pārvaldība

1. Mērķis

1.1 Šī politika nosaka minimālos obligātos lietojumprogrammu drošības kontroles pasākumus, kas jāpiemēro visiem programmatūras un sistēmu risinājumiem, kurus organizācija izmanto, neatkarīgi no tā, vai tie ir izstrādāti iekšēji vai iegādāti no ārējiem piegādātājiem.

1.2 Tā nodrošina, ka lietojumprogrammas tiek projektētas, ieviestas un uzturētas tā, lai aizsargātu klientu, darbinieku un organizācijas datus pret nesankcionētu piekļuvi, neatbilstošu izmantošanu, izmainīšanu vai iznīcināšanu.

1.3 Šī politika atbalsta organizācijas centienus iegūt un uzturēt ISO/IEC 27001 sertifikāciju, izpildīt VDAR un NIS2 prasības un samazināt darbības riskus, kas saistīti ar nedrošu programmatūras izvietošanu.

1.4 Tā palīdz izveidot konsekventu un auditējamu pieeju lietojumprogrammu drošībai MVU vidē, nosakot vienotu drošības funkciju un prakšu kontrolsarakstu, kas pielāgots vidēm ar ierobežotiem iekšējiem tehniskajiem resursiem.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām lietojumprogrammām, sistēmām, rīkiem un platformām, kas:

2.1.1 tiek izstrādātas iekšēji, pielāgotas vai skriptētas iekšējai lietošanai;

2.1.2 tiek iegādātas kā komerciāla programmatūra, SaaS vai mākoņpakalpojumi;

2.1.3 apstrādā, glabā vai pārsūta personas datus, organizācijas ierakstus vai sensitīvu darbības informāciju;

2.1.4 ir pieejamas darbiniekiem, līgumslēdzējiem, klientiem vai partneriem, izmantojot iekšējos tīklus, internetu vai mobilās platformas.

2.2 Politika attiecas uz:

2.2.1 izstrādātājiem (iekšējiem vai ārpakalpojuma sniedzējiem);

2.2.2 programmatūras piegādātājiem un mākoņpakalpojumu sniedzējiem;

2.2.3 IT atbalsta personālu vai administratoriem, kas atbild par ieviešanu un atbalstu;

2.2.4 lietojumprogrammu īpašniekiem un biznesa lietotājiem, kuri iesaistīti sistēmu apstiprināšanā un uzraudzībā.

3. Mērķi

3.1 Nodrošināt, ka visām organizācijas izmantotajām lietojumprogrammām ir iebūvēti un pārbaudāmi drošības kontroles pasākumi, kas mazina izplatītas programmatūras ievainojamības.

3.2 Aizsargāt lietojumprogrammu apstrādāto datu konfidencialitāti, integritāti un pieejamību neatkarīgi no to izvietošanas vietas.

3.3 Noteikt prasību veikt formālu lietojumprogrammu drošības testēšanu, pārskatīšanu un validāciju pirms jebkuras jaunas lietojumprogrammas vai būtiska atjauninājuma apstiprināšanas lietošanai produkcijas vidē.

3.4 Nodrošināt konsekventu un drošu lietotāju autentifikācijas datu, sesiju datu un piekļuves tiesību apstrādi visās darbībai kritiskajās sistēmās.

3.5 Noteikt prasību, ka visām lietojumprogrammām jānodrošina droša žurnalēšana, auditējamība un uzraudzības funkcijas, lai atbalstītu aizdomīgu darbību identificēšanu un reaģēšanu uz tām.

3.6 Samazināt juridiskos un atbilstības riskus, nodrošinot, ka lietojumprogrammas atbilst piemērojamajām normatīvajām drošības prasībām.

4. Lomas un pienākumi

4.1 Ģenerāldirektors (GM)

4.1.1 Uzņemas vispārējo atbildību par lietojumprogrammu drošību visā organizācijā.

4.1.2 Apstiprina šo politiku un nodrošina, ka visas iegādes vai izstrādes iniciatīvas atbilst tās prasībām.

4.1.3 Nodrošina, ka piegādātāju un pakalpojumu sniedzēju līgumos ir ietvertas lietojumprogrammu drošības prasības.

4.1.4 Pārskata un apstiprina riska izņēmumus, ja pilnīgu atbilstību nav iespējams nodrošināt darbības ierobežojumu dēļ.

4.2 Lietojumprogrammas īpašnieks (ja ir norīkots)

4.2.1 Nosaka lietojumprogrammai specifiskās drošības vajadzības sistēmas izvēles vai projekta uzsākšanas laikā.

4.2.2 Pārbauda, vai ir iekļautas galvenās funkcijas, piemēram, pieteikšanās aizsardzība, šifrēšana un darbību žurnalēšana.

4.2.3 Piedalās pirmsieviešanas pārskatīšanā un apstiprina, ka drošības kontroles pasākumi atbilst darbības vajadzībām.

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

9. Pārskatīšanas un atjaunināšanas prasības

9.1 Šī politika ģenerāldirektoram jāpārskata vismaz reizi kalendārajā gadā, lai:

9.1.1 atspoguļotu izmaiņas normatīvajās prasībās (piemēram, VDAR, NIS2, DORA);

9.1.2 iekļautu jaunus vai pieaugošus apdraudējumus un uzbrukumu paņēmienus;

9.1.3 atjauninātu formulējumus un prasības atbilstoši izmaiņām platformās, piegādātājos vai izstrādes metodēs.

9.2 Starpposma pārskatīšana jāveic arī tad, ja:

9.2.1 tiek ieviestas jaunas lietojumprogrammas;

9.2.2 esošajām lietojumprogrammām tiek veikti būtiski atjauninājumi vai integrācija;

9.2.3 notiek ar lietojumprogrammu saistīts incidents vai pārkāpums;

9.2.4 tiek identificēti jauni riski, pamatojoties uz ārējiem paziņojumiem vai nozares brīdinājumiem.

9.3 Visi šīs politikas atjauninājumi:

9.3.1 jāapstiprina ģenerāldirektoram;

9.3.2 jādokumentē, norādot versiju vēsturi un izmaiņu pamatojumu;

9.3.3 jāpaziņo visiem darbiniekiem, izstrādātājiem un piegādātājiem, kuri iesaistīti lietojumprogrammu pārvaldībā;

9.3.4 droši jāuzglabā audita un atbilstības vajadzībām.

10. Saistītās politikas un sasaiste

10.1 Šo politiku tieši atbalsta un tās ieviešanu nodrošina šādas MVU vajadzībām pielāgotas drošības politikas:

10.1.1 P2S – Pārvaldības lomu un atbildības politika: nosaka atbildību par lietojumprogrammu apstiprināšanu, politikas ievērošanas nodrošināšanu un piegādātāju pārvaldību.

10.1.2 P4S – Piekļuves kontroles politika: nodrošina, ka piekļuve lietojumprogrammām atbilst minimālo privilēģiju principam un sesiju kontroles principiem.

10.1.3 P8S – Informācijas drošības informētības un apmācības politika: nodrošina, ka lietotāji un izstrādātāji ir apmācīti atpazīt un ziņot par ar lietojumprogrammām saistītiem apdraudējumiem.

10.1.4 P17S – Datu aizsardzības un privātuma politika: nosaka datu privātuma drošības pasākumus, kas jāpiemēro jebkurai lietojumprogrammai, kura apstrādā personas informāciju.

10.1.5 P14S – Datu uzglabāšanas politika: regulē, kā lietojumprogrammu ģenerētie žurnāli, rezerves kopijas un sensitīvie dati jāglabā, jāarhivē un droši jāiznīcina.

10.1.6 P30S – Incidentu reaģēšanas politika: nosaka darbības ar lietojumprogrammām saistītu drošības notikumu identificēšanai, ziņošanai un ierobežošanai.

10.2 Kopā šīs politikas nodrošina, ka lietojumprogrammu drošība ir pilnībā integrēta organizācijas informācijas drošības pārvaldības sistēmā un ir auditējama.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8. punkts – nosaka prasību organizācijām ieviest darbības kontroles pasākumus informācijas drošības risku pārvaldībai, tostarp risku, kas saistīti ar lietojumprogrammām un programmatūras sistēmām, pārvaldībai.

11.2 ISO/IEC 27002

11.2.1 8.25. kontrole – paredz drošas projektēšanas, izstrādes un koda pārskatīšanas prakšu ieviešanu visām lietojumprogrammām, tostarp tām, ko nodrošina piegādātāji.

11.2.2 8.26. kontrole – paredz formālu lietojumprogrammu drošības kontroles pasākumu testēšanu, jo īpaši piekļuves kontroles, ievades validācijas un sesiju apstrādes jomās.

11.3 NIST SP 800-53 Rev.5

11.3.1 SA-11 – nosaka prasības izstrādātāju testēšanai, koda analīzei un dinamiskajai lietojumprogrammu skenēšanai pirms ieviešanas.

11.3.2 SI-10 – attiecas uz izplatītu programmatūras trūkumu identificēšanu un novēršanu, uzsverot izstrādātāju informētību un tehniskos drošības pasākumus.

11.4 ES VDAR (2016/679)

11.4.1 25. pants – “datu aizsardzība pēc noklusējuma un integrēti pēc projektēšanas” nosaka pienākumu iestrādāt privātuma un drošības prasības lietojumprogrammu, kas apstrādā personas datus, pamatprojektējumā.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 21. panta 2. punkta a) un e) apakšpunkts – nosaka prasību būtiskām un svarīgām struktūrām ieviest tehniskos pasākumus lietojumprogrammu aizsardzībai un ar programmatūru saistīto risku identificēšanai.

11.6 ES DORA (2022/2554)

11.6.1 9. panta 2. punkta c) apakšpunkts, 10. panta 2. punkta c) apakšpunkts – nosaka prasību finanšu sektora MVU iestrādāt lietojumprogrammu līmeņa drošības kontroles pasākumus un veikt regulāru izvērtēšanu digitālās darbības noturības uzturēšanai.

11.7 COBIT 2019

11.7.1 BAI03 – “Risinājumu identificēšanas un izveides pārvaldība” sniedz vadlīnijas drošas programmatūras izstrādei vai iegādei atbilstoši riskam, atbilstības prasībām un darbības vajadzībām, arī MVU vidē ar ierobežotiem resursiem.