					Šeit ievadiet reģistrētās juridiskās personas nosaukumu							
Dokumenta numurs: P22					Dokumenta nosaukums: **Žurnālfiksēšanas un uzraudzības 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 Šīs politikas mērķis ir noteikt skaidras un izpildāmas prasības žurnālu veidošanai, aizsardzībai, pārskatīšanai un analīzei, lai visā organizācijas IT vidē reģistrētu būtiskākos sistēmu un drošības notikumus.

1.2 Audita žurnālu veidošana un uzraudzība ir būtiska anomāliju noteikšanai, reaģēšanai uz apdraudējumiem, kriminālistiskajai izmeklēšanai, gatavībai auditam un normatīvo aktu prasību ievērošanai. Šī politika nodrošina, ka visi sistēmu ģenerētie notikumi tiek pienācīgi reģistrēti, glabāti un korelēti, izmantojot laika ziņā sinhronizētus un precīzus datus.

1.3 Šī politika ir būtiska, lai atbalstītu ISO/IEC 27001 8. punktu un A pielikuma 8.15. kontroles pasākumu (Žurnālfiksēšana), 8.16. kontroles pasākumu (Uzraudzība) un 8.17. kontroles pasākumu (Pulksteņu sinhronizācija), kā arī tā ir tieši saistīta ar normatīvajiem pienākumiem saskaņā ar GDPR, NIS2, DORA un COBIT 2019.

2. Piemērošanas joma

2.1 Šī politika attiecas uz visām sistēmām, pakalpojumiem un vidēm, kurās tiek glabāti, apstrādāti vai pārsūtīti dati, kas ietilpst informācijas drošības pārvaldības sistēmas darbības jomā, tai skaitā:

2.1.1 lokālo infrastruktūru, mākoņpakalpojumus (piemēram, IaaS, PaaS, SaaS) un hibrīdvides;

2.1.2 operētājsistēmas, datubāzes, lietotnes un tīkla iekārtas;

2.1.3 drošības sistēmas, piemēram, SIEM, ugunsmūrus, EDR platformas, VPN koncentratorus un identitātes nodrošinātājus.

2.2 Piemērošanas jomā ietilpst šādas iesaistītās puses:

2.2.1 iekšējie lietotāji ar sistēmas vai administratīvajām privilēģijām;

2.2.2 infrastruktūras un IT operāciju personāls;

2.2.3 drošības operāciju centrs (SOC) un apdraudējumu noteikšanas komandas;

2.2.4 programmatūras izstrādātāji un lietotņu īpašnieki;

2.2.5 trešo pušu pakalpojumu sniedzēji, kuri pārvalda sistēmas, kas ģenerē žurnālus.

3. Mērķi

3.1 Nodrošināt, ka visas kritiski svarīgās sistēmas ģenerē drošības notikumu žurnālus un sistēmas darbību ierakstus, kas tiek glabāti atbilstoši normatīvajām, juridiskajām un līgumiskajām prasībām.

3.2 Noteikt minimālos notikumu veidus un žurnālu saturu, kas nepieciešams, lai atklātu nesankcionētas darbības, izsekotu lietotāju darbības un atbalstītu kriminālistisko izmeklēšanu.

3.3 Nodrošināt aizsardzības pasākumus, lai nepieļautu manipulācijas ar žurnāliem, nesankcionētu dzēšanu vai nekontrolētu piekļuvi žurnālu datiem.

3.4 Ieviest centralizētas žurnālfiksēšanas un brīdināšanas sistēmas (piemēram, SIEM), lai apkopotu, korelētu un eskalētu aizdomīgas darbības gandrīz reāllaikā.

3.5 Nodrošināt sistēmu pulksteņu sinhronizāciju, lai būtu iespējama precīza starpsistēmu korelācija un incidentu analīze.

3.6 Nodrošināt nepārtrauktu pilnveidi un atbilstību, integrējot žurnālu uzraudzību ar audita, risku un incidentu pārvaldības procesiem.

4. Lomas un pienākumi

4.1 Galvenais informācijas drošības vadītājs (CISO)

4.1.1 Ir šīs politikas īpašnieks un nodrošina, ka tā atbilst organizācijas riska profilam, audita prasībām un IDPS pienākumiem.

4.1.2 Apstiprina žurnālfiksēšanas tvērumu reglamentētām vai augsta riska sistēmām un pārrauga atbilstības ziņošanu.

4.2 Drošības operāciju centra (SOC) vadītājs

4.2.1 Pārvalda un uztur centralizētās žurnālu pārvaldības platformas (piemēram, SIEM).

4.2.2 Nosaka žurnālu apkopošanas noteikumus, brīdinājumu sliekšņus un incidentu triāžas eskalācijas ceļus.

4.2.3 Katru dienu pārskata atskaites un nodrošina, ka anomālijas tiek analizētas, dokumentētas un, ja nepieciešams, eskalētas.

[... 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 agrāk, ja notiek:

9.1.1 būtiskas izmaiņas sistēmu arhitektūrā vai žurnālfiksēšanas infrastruktūrā (piemēram, SIEM migrācija);

9.1.2 izmaiņas normatīvajās žurnālfiksēšanas prasībās (piemēram, NIS2, DORA žurnālfiksēšanas pienākumi);

9.1.3 auditu konstatējumi vai pēcincidenta izvērtējumu rezultāti;

9.1.4 jauni apdraudējumi, kuru dēļ nepieciešama pastiprināta uzraudzība (piemēram, iekšējie apdraudējumi, kompromitācija piegādes ķēdē).

9.2 Pārskatīšanas procesu vada Drošības operāciju centra (SOC) vadītājs sadarbībā ar CISO, risku pārvaldības, atbilstības un IT infrastruktūras komandām.

9.3 Apstiprinātās izmaiņas jāpārvalda, izmantojot versiju kontroli IDPS dokumentu kontroles reģistrā, un par tām jāpaziņo:

9.3.1 visām iesaistītajām pusēm, kuru atbildībā ir žurnālfiksēšanas sistēmu uzturēšana;

9.3.2 lietotņu un sistēmu īpašniekiem;

9.3.3 trešo pušu pakalpojumu sniedzējiem, kuriem ir pienākumi saistībā ar telemetriju vai SIEM integrāciju.

9.4 Visas aizstātās versijas droši jāarhivē, piekļuvi tām ierobežojot tikai autorizētiem IDPS pārziņiem audita un juridiskiem mērķiem.

10. Saistītās politikas un sasaiste

10.1 P1 – Informācijas drošības politika. Tā nosaka pamatapņemšanos aizsargāt sistēmas un datus, kuras ietvaros žurnālfiksēšana un uzraudzība kalpo kā būtiski atklājošie kontroles pasākumi un reaģēšanas atbalsta mehānismi.

10.2 P4 – Piekļuves kontroles politika. Tā nodrošina, ka privileģētās piekļuves, lietotāju pieteikšanās un autorizācijas notikumi tiek reģistrēti žurnālos un uzraudzīti, lai atklātu ļaunprātīgu izmantošanu vai anomālu uzvedību.

10.3 P5 – Izmaiņu pārvaldības politika. Tā nosaka pienākumu reģistrēt žurnālos sistēmu izmaiņas, ielāpu ieviešanu un konfigurācijas atjauninājumus, kas var radīt risku vai izraisīt nesankcionētas izmaiņas.

10.4 P21 – Tīkla drošības politika. Tā nosaka tīkla līmeņa žurnālfiksēšanu (piemēram, ugunsmūra žurnālus, IDS/IPS brīdinājumus, VPN darbību) un integrāciju ar SIEM, lai nodrošinātu redzamību datplūsmas anomālijās un perimetra aizsardzībā.

10.5 P23 – Laika sinhronizācijas politika. Tā nodrošina pulksteņu konsekvenci visās sistēmās, kas ir būtiski uzticamai žurnālfiksēšanai un drošības notikumu korelācijai vairākās vidēs.

10.6 P30 – Incidentu reaģēšanas politika. Tā balstās uz žurnālu datiem un brīdināšanas mehānismiem, lai identificētu, izmeklētu un novērstu drošības incidentus, vienlaikus saglabājot kriminālistiskos artefaktus pēcincidenta pārskatīšanai.

11. Atsauces standarti un ietvari

11.1 ISO/IEC 27001

11.1.1 8. punkts – Darbības plānošana un kontrole: nosaka prasību ieviest kontroles pasākumus darbību uzraudzībai un aizsardzībai pret nesankcionētu piekļuvi un sistēmu neatbilstošu izmantošanu.

11.2 ISO/IEC 27002:2022 – 8.15., 8.16. un 8.17. kontroles pasākumi

11.2.1 Nosaka detalizētas žurnālfiksēšanas prasības, tai skaitā kādi notikumi jāreģistrē, kā aizsargāt un analizēt žurnālus un kā nodrošināt laikspiedolu uzticamību visās sistēmās.

11.3 NIST SP 800-53 Rev. 5

11.3.1 AU-2 līdz AU-12: aptver notikumu atlasi, žurnālfiksēšanu, aizsardzību, audita pārskatīšanu, reaģēšanu uz audita kļūmēm un audita ierakstu glabāšanu.

11.3.2 SI-4 – Sistēmu uzraudzība: nosaka prasību aktīvi uzraudzīt sistēmas, izmantojot brīdinājumus, kas balstīti uz anomālu darbību.

11.3.3 SC-45 – Sistēmas laika sinhronizācija: nostiprina laika precizitātes prasību notikumu izsekojamībai un incidentu korelācijai.

11.4 ES GDPR (2016/679)

11.4.1 32. pants – apstrādes drošība: nosaka tehniskus kontroles pasākumus, piemēram, žurnālfiksēšanu un uzraudzību, lai nodrošinātu drošību un pārskatatbildību, īpaši attiecībā uz piekļuvi personas datiem.

11.5 ES NIS2 direktīva (2022/2555)

11.5.1 21. panta 2. punkta e) apakšpunkts: nosaka pienākumu ieviest notikumu žurnālfiksēšanas un uzraudzības sistēmas drošības incidentu ātrai noteikšanai un reaģēšanai uz tiem.

11.6 ES DORA (2022/2554)

11.6.1 9. pants – IKT risku pārvaldība: nosaka prasību ieviest mehānismus anomālu darbību noteikšanai, incidentu reģistrēšanai žurnālos un kriminālistisko datu glabāšanai.

11.6.2 11. pants – IKT darbības nepārtrauktības plānu testēšana: uzsver uzraudzības nepārtrauktību un žurnālu pieejamības validēšanu darbības traucējumu laikā.

11.7 COBIT 2019

11.7.1 DSS01.05 – Drošības žurnālu pārvaldība: nosaka prasību ieviest žurnālfiksēšanas iespējas visai kritiskajai infrastruktūrai.

11.7.2 DSS05.04 – Drošības notikumu uzraudzība: nosaka prasību reāllaikā uzraudzīt un analizēt žurnālus, lai noteiktu notikumus un reaģētu uz tiem.

11.7.3 MEA03 – Atbilstības uzraudzība, izvērtēšana un novērtēšana: nosaka prasību regulāri pārskatīt žurnālfiksēšanas praksi un tās atbilstību kontroles mērķiem.