| | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | | | | | Šeit ievadiet reģistrētās juridiskās personas nosaukumu | | | | | | | |
| Dokumenta numurs:<br>P22S | | | | | Dokumenta nosaukums:<br>**Žurnālfiksēšanas un uzraudzības politika** | | | | | | | |
| Versija:<br>1.0 | | Spēkā stāšanās datums:<br>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. sadaļa | Darbības kontroles pasākumi, tostarp žurnālfiksēšana |
| ISO/IEC 27002:2022 | Kontroles pasākumi 8.15, 8.16, 8.17 | Notikumu žurnālfiksēšana, aizsardzība un uzraudzība |
| NIST SP 800-53 Rev.5 | AU-2 līdz AU-12, SI-4 | Audita žurnālu saturs un pārskatīšana, glabāšana, anomāliju noteikšana un brīdināšana |
| ES GDPR | 5. panta 1. punkta f) apakšpunkts, 32. un 33. pants | Personas datu konfidencialitāte un integritāte, tehniskie pasākumi un paziņošana par pārkāpumiem |
| ES NIS2 | 21. panta 2. punkta d) apakšpunkts, 23. pants | Žurnalēšanas mehānismi anomāliju noteikšanai un ziņošanai par incidentiem 24 stundu laikā |
| ES DORA | 10. un 15. pants | Operacionālā noturība, pakalpojumu sniedzēju uzraudzība un žurnālfiksēšana |
| COBIT 2019 | DSS01.03, DSS05.02 | Darbību izsekojamība un aizsardzība, izmantojot žurnālfiksēšanu un uzraudzību |

**1. Mērķis**

1.1 Šī politika nosaka obligātos audita žurnālu veidošanas un uzraudzības kontroles pasākumus, lai nodrošinātu organizācijas IT sistēmu drošību, pārskatatbildību un darbības integritāti.

1.2 Tā nosaka, kāda veida notikumi ir jāreģistrē žurnālos, kā žurnāli tiek glabāti, kā tie tiek pārskatīti un kādi ir personāla un pakalpojumu sniedzēju pienākumi.

1.3 Žurnālfiksēšana un uzraudzība atbalsta apdraudējumu noteikšanu, regulatīvo atbilstību, reaģēšanu uz incidentiem un kriminālistisko analīzi.

1.4 Šī politika ļauj organizācijai izpildīt ISO/IEC 27001 darbības kontroles prasības un atbalsta pastāvīgu gatavību auditam, klientu uzticēšanos un atbilstību GDPR, NIS2 un DORA prasībām.

**2. Piemērošanas joma**

**2.1 Šī politika attiecas uz visām organizācijas sistēmām un lietotājiem, tostarp:**

2.1.1 darbstacijām, klēpjdatoriem, serveriem, ugunsmūriem, komutatoriem, maršrutētājiem un bezvadu piekļuves punktiem;

2.1.2 mākoņpakalpojumiem, ko izmanto saimnieciskās darbības nodrošināšanai (piemēram, e-pastam, failu glabāšanai, rezerves kopijām, sadarbības rīkiem);

2.1.3 žurnālfiksēšanas funkcijām pretvīrusu programmatūrā, lietotnēs, operētājsistēmās un tīkla iekārtās;

2.1.4 visiem darbiniekiem, līgumslēdzējiem un pārvaldīto pakalpojumu sniedzējiem (MSP), kuri izmanto vai administrē sistēmas;

2.1.5 jebkuru vidi, kurā tiek izmantotas organizācijas IT sistēmas, tostarp attālinātā darba, hibrīddarba vai BYOD vidēs.

2.2 Politika attiecas arī uz žurnāliem, ko ģenerē trešo pušu pakalpojumi, ja organizācijai ir administratīvā piekļuve vai audita tiesības atbilstoši līgumam.

**3. Mērķi**

3.1 Nodrošināt sistēmu darbību žurnālfiksēšanu, tostarp autentifikāciju, konfigurācijas izmaiņas, piekļuvi sensitīviem datiem un drošības brīdinājumus.

3.2 Uzturēt drošus un precīzus žurnālus, lai atklātu politikas pārkāpumus, sistēmu kļūdas vai nesankcionētas darbības.

3.3 Nodrošināt iespēju operatīvi pārskatīt žurnālus incidentu, izmeklēšanu un auditu laikā.

3.4 Atbalstīt laika sinhronizāciju, lai nodrošinātu žurnālu datu integritāti un savstarpējo korelāciju.

3.5 Aizsargāt žurnālus pret manipulācijām, zudumu vai priekšlaicīgu dzēšanu.

3.6 Izpildīt tiesiskos un regulatīvos pienākumus attiecībā uz sistēmu pārskatatbildību, izsekojamību un reaģēšanu uz pārkāpumiem.

**4. Lomas un pienākumi**

**4.1 Ģenerāldirektors (GM)**

4.1.1 Apstiprina šo politiku un nodrošina tās ieviešanu visās organizācijas pamatdarbības sistēmās.

4.1.2 Pārskata augstas smaguma pakāpes brīdinājumus un būtiskus audita konstatējumus, par kuriem ziņo IT vai datu aizsardzības funkcija.

4.1.3 Apstiprina izņēmumus, ja žurnālfiksēšanu vai glabāšanu tehniski nav iespējams nodrošināt.

**4.2 IT atbalsta pakalpojumu sniedzējs / iekšējā IT funkcija**

4.2.1 Ievieš un konfigurē žurnālfiksēšanu operētājsistēmām, tīkla iekārtām, pretvīrusu rīkiem un būtiskajām lietotnēm.

4.2.2 Nodrošina, ka žurnāli tiek glabāti, iekļauti rezerves kopijās un aizsargāti pret izmaiņām.

4.2.3 Pārskata žurnālus saskaņā ar noteikto grafiku un izmeklē aizdomīgas vai nesankcionētas darbības.

4.2.4 Uztur brīdināšanas mehānismus, kas identificē anomālu uzvedību vai ielaušanās indikatorus.

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

**9. Pārskatīšanas un atjaunināšanas prasības**

**9.1 Ikgadējā pārskatīšana**

9.1.1 Šī politika jāpārskata vismaz reizi gadā ģenerāldirektoram ar IT atbalsta pakalpojumu sniedzēja un privātuma koordinatora atbalstu.

**9.2 Pārskatīšanas ierosinātāji**

**9.2.1 Neplānota pārskatīšana jāveic, reaģējot uz:**

9.2.1.1 ar žurnāliem saistītiem konstatējumiem iekšējos vai ārējos auditos;

9.2.1.2 drošības incidentiem, kuros žurnāli bija trūkstoši, bojāti vai nepietiekami;

9.2.1.3 būtiskām izmaiņām IT infrastruktūrā (piemēram, migrācijai uz mākoņvides žurnālfiksēšanas platformām);

9.2.1.4 izmaiņām tiesiskajos vai regulatīvajos pienākumos (piemēram, GDPR, NIS2, DORA).

**9.3 Versiju kontrole**

9.3.1 Visas izmaiņas šajā politikā jāreģistrē, norādot versijas numuru, datumu un grozījumu kopsavilkumu.

9.3.2 Iepriekšējās versijas jāarhivē un jāglabā vismaz 3 gadus.

9.3.3 Atjauninātās politikas jāpaziņo ietekmētajām iesaistītajām pusēm, īpaši tiem, kuriem ir sistēmu līmeņa piekļuve.

## 10. Saistītās politikas un sasaiste

### 10.1 Šī politika tieši atbalsta turpmāk minētās MVU informācijas drošības politikas un ir ar tām savstarpēji saistīta:

10.1.1 P17S – Datu aizsardzības un privātuma politika: nodrošina, ka žurnālu dati, kas satur personas informāciju, tiek pārvaldīti ar integritātes, glabāšanas un piekļuves aizsardzības pasākumiem atbilstoši GDPR prasībām.

10.1.2 P21S – Tīkla drošības politika: nodrošina pamatu ar ugunsmūriem, bezvadu piekļuvi, VPN un segmentēšanas uzraudzību saistīto žurnālu iegūšanai.

10.1.3 P24S – Drošas izstrādes politika: nodrošina, ka lietotņu žurnāli (piemēram, pieteikšanās mēģinājumi, kļūdas un izņēmumi) tiek iekļauti programmatūras projektēšanā un ekspluatācijā.

10.1.4 P30S – Incidentu reaģēšanas politika: balstās uz precīziem un pilnīgiem žurnālu datiem, lai noteiktu, analizētu un apstrādātu informācijas drošības notikumus.

10.1.5 P23S – Laika sinhronizācijas politika: nodrošina konsekventus un izsekojamus laikspiedolus visās sistēmās, ļaujot korelēt žurnālus izmeklēšanu laikā.

## 11. Atsauces standarti un ietvari

### 11.1 ISO/IEC 27001

11.1.1 8. sadaļa – nosaka prasību ieviest darbības kontroles pasākumus informācijas drošības risku mazināšanai, tostarp žurnālfiksēšanu.

### 11.2 ISO/IEC 27002

11.2.1 8.15. kontrole – nosaka notikumu žurnālfiksēšanu, lai atbalstītu anomāliju noteikšanu un pārskatatbildību.

11.2.2 8.16. kontrole – nosaka žurnālu aizsardzību pret manipulācijām un nesankcionētu piekļuvi.

11.2.3 8.17. kontrole – nosaka sistēmu uzraudzību neparastas aktivitātes noteikšanai un uzraudzības kontroles pasākumu efektivitātes apstiprināšanai.

### 11.3 NIST SP 800-53 Rev.5

11.3.1 AU-2 līdz AU-12 – aptver audita žurnālu saturu, pārskatīšanu, glabāšanu un automātisku brīdināšanu.

11.3.2 SI-4 – nosaka sistēmu anomāliju noteikšanu un ziņošanu par aizdomīgiem notikumiem.

### 11.4 ES GDPR

11.4.1 5. panta 1. punkta f) apakšpunkts – nosaka personas datu integritāti un konfidencialitāti, tostarp piekļuves žurnālfiksēšanu.

11.4.2 32. pants – nosaka tehniskus un organizatoriskus pasākumus drošības nodrošināšanai, tostarp žurnālfiksēšanu un uzraudzību.

11.4.3 33. pants – nosaka savlaicīgu paziņošanu par pārkāpumiem, ko atbalsta žurnāli, kuri ļauj veikt pamatcēloņa analīzi.

### 11.5 ES NIS2 direktīva

11.5.1 21. panta 2. punkta d) apakšpunkts – nosaka žurnalēšanas mehānismus, kas identificē anomālijas un atbalsta incidentu izmeklēšanu.

11.5.2 23. pants – nosaka pienākumu ziņot par incidentiem 24 stundu laikā, kas ir atkarīgs no precīziem un savlaicīgiem žurnālu datiem.

### 11.6 ES DORA

11.6.1 10. pants – nosaka digitālās darbības noturības prasības, tostarp ar IKT saistītu incidentu izsekojamību, izmantojot žurnālfiksēšanu.

11.6.2 15. pants – nosaka pienākumu uzraudzīt pakalpojumu sniedzējus, tostarp nodrošinot piekļuvi žurnāliem un to pārskatīšanas tiesības.

**11.7 COBIT 2019**

11.7.1 DSS01.03 – nosaka sistēmu darbību izsekojamību, izmantojot žurnālfiksēšanu un uzraudzību.

11.7.2 DSS05.02 – nosaka žurnālfiksēšanu kā būtisku kontroles pasākumu aizsardzībai pret ļaunatūru un citām nesankcionētām darbībām.