Nacionālais kiberdrošības centrs

https://cyber.gov.lv, NIS2@mod.gov.lv, 67335131

Žurnālfailu vadlīnijas

Saskaņā ar Ministru kabineta 2025. gada
25. jūnija noteikumiem Nr. 397

Šīs vadlīnijas izstrādātas Nacionālās kiberdrošības likuma subjektiem (būtisko pakalpojumu sniedzējiem, svarīgo pakalpojumu sniedzējiem un IKT kritiskās infrastruktūras īpašniekiem).

Izstrādātājs – CERT.LV

Versija 1.0, 07.01.2026

SATURS

1. IEVADS

Žurnālfaili (angļu valodā - *audit logs* vai *log files*) ir strukturēti ieraksti, kas automātiski fiksē dažādu notikumu informāciju (piemēram, piekļuve, datu ievade, maiņa, dzēšana, lejupielāde) informācijas sistēmās, tīkla iekārtās un citās IKT infrastruktūras sastāvdaļās. Tie satur būtisku informāciju par piekļuves mēģinājumiem, lietotāju darbībām, sistēmas izmaiņām, kļūdām un citiem nozīmīgiem notikumiem, kas ir svarīgi gan drošības uzraudzībai, gan sistēmu darbības analīzei, incidentu izmeklēšanai un atbilstības pārbaudei.

Žurnālfailu veidošana ir neatņemama daļa no informācijas drošības pārvaldības, jo tie sniedz pierādāmu notikumu vēsturi un palīdz identificēt potenciālos apdraudējumus, ļaunprātīgu rīcību vai sistēmas darbības traucējumus. Atbilstoša žurnālfailu pārvaldība palīdz nodrošināt arī organizācijas atbilstību normatīvajiem aktiem, industrijas standartiem un iekšējām drošības prasībām.

Šīs rekomendācijas ir paredzētas, lai sniegtu atbalstu par žurnālfailu veidošanu atbildīgajām personām, veidot un uzturēt efektīvu žurnālfailu pārvaldības kārtību. Šajās rekomendācijās turpmāk apskatīti šādi aspekti:

- žurnālfailu veidošanas mērķi;
- žurnālfailu veidošanas tiesiskais regulējums;
- žurnālfailu pārvaldības principi un pārvaldības politikas prasības;
- notikumu veidi, kurus nepieciešams reģistrēt informācijas sistēmās, tīkla un VPN iekārtās;
- žurnālfailu aizsardzības un integritātes nodrošināšana;
- žurnālfailu analīzes, glabāšanas un arhivēšanas prasības.

Rekomendācijas, kuras sniegtas šajā dokumentā, nav uzskatāmas par obligātām un to ieviešana nedrīkst būt pretrunā ar organizācijai saistošajiem normatīvajiem aktiem, standartiem vai vadlīnijām, kuras noteiktas organizācijai kā obligātas.

2. ŽURNĀLFAILU MĒRĶIS

Žurnālfailu veidošana un pārvaldība ir vērsta uz to, lai nodrošinātu organizācijas IKT resursu pārskatāmību, drošību un pārvaldību. Žurnālfaili kalpo kā būtisks informācijas avots, kas ļauj organizācijai pieņemt datos pamatotus lēmumus un reaģēt uz drošības riskiem.

Žurnālfailu galvenie mērķi ir šādi:

- Sniegt pārskatu par organizācijas IKT resursu darbībām, lai varētu veikt plānotus un ar drošības uzlabošanu saistītus soļus, atvieglotu infrastruktūras uzraudzību;
- Nodrošināt iespēju identificēt nesankcionētas piekļuves IKT resursiem vai citas ļaunprātīgas darbības;
- Nodrošināt iespēju atklāt, izmeklēt kiberapdraudējumus un kiberincidentus;
- Nodrošināt pierādāmu notikumu apskatu, kas var kalpot kā pierādījumi auditam, iekšējām pārbaudēm vai kiberincidenta izmeklēšanai, tai skaitā, iesniegšanai kompetentajām iestādēm;

- Nodrošināt atbilstību organizācijai piemērojamām prasībām, kuras noteiktas normatīvajos aktos, standartos vai vadlīnijās un kas paredz žurnālfailu reģistrāciju vai spēju identificēt kiberapdraudējumus.

3. NORMATĪVIE AKTI

Dažādām organizācijām ir saistoši atšķirīgi normatīvie akti, standarti un labās prakses prasības, kas tieši vai netieši ietekmē žurnālfailu pārvaldības politiku. Katrai organizācijai ir jāidentificē, kuri no šiem dokumentiem tai ir piemērojami, un jānodrošina atbilstība to prasībām.

Viens no būtiskākajiem ārējiem normatīvajiem aktiem kiberdrošības jomā, kas aptver plašu organizāciju loku, ir Nacionālās kiberdrošības likums (turpmāk – NKDL). No šī likuma izriet vairāki Ministru Kabineta noteikumi, tostarp 2025.gada 25.jūnija Ministru kabineta noteikumi Nr.397 "*Minimālās kiberdrošības prasības*" (turpmāk – MK Nr.397), kas tieši nosaka arī prasības attiecībā uz žurnālfailu pārvaldību NKDL subjektiem.

MK Nr.397 3.9. apakšsadaļa nosaka vairākas prasības NKDL subjektiem saistībā ar žurnālfailiem, tai skaitā, cik ilgu laiku ir jāuzglabā žurnālfaili, par kādiem notikumiem ir jāveido žurnālfaili, kā tos fiksēt, u.tml. Tāpat MK Nr.397 nosaka, ka IKT kritiskās infrastruktūras īpašniekam vai tiesiskajam valdītājam ir jānosaka par žurnālfailu pārvaldību atbildīgo personu, un par to ir jāpaziņo Satversmes aizsardzības birojam. Tai pašā laikā ir jāņem vērā, ka MK Nr.397 20.punktā tiek noteikts, ka IKT kritiskā infrastruktūrā kiberdrošības pārvaldnieks vienlaikus nevar būt atbildīgā persona par žurnālfailu pārvaldību.

Lai arī šīs rekomendācijas ir veidotas, balstoties uz MK Nr.397 noteiktajām prasībām NKDL subjektiem, arī citas organizācijas – neatkarīgi no juridiskā statusa vai nozares – var gūt būtisku ieguvumu no šo rekomendāciju ievērošanas, jo tās veicina labu praksi informācijas drošības pārvaldībā.

4. ŽURNĀLFAILU PĀRVALDĪBA

Žurnālfailu pārvaldību nepieciešams regulāri pārskatīt un atjaunot atbilstoši tā brīža situācijai, bet ne retāk kā reizi gadā, lai nodrošinātu atbilstību organizācijas vajadzībām, normatīvajiem aktiem, standartiem un labajām praksēm.

- *Politikas atjaunošana* – pēc nepieciešamības, bet ne retāk kā reizi gadā pārskatīt organizācijas žurnālfailu pārvaldības politiku;
- *Žurnālfailu pārskatīšana* – var tikt veikta automatizēti vai manuāli, brīžos, kad automatizēta pieeja nespēj sasniegt vēlamo rezultātu, piemēram, ja ir atklātas tādas uzbrukuma, ievainojamības vai citas informācijas sistēmu apdraudošas pazīmes, kuras automatizēta pieeja nespēja atklāt. Regulāri, bet ne retāk kā reizi gadā, jāveic uzkrātās informācijas analīze, lai identificētu aizdomīgas darbības un neatbilstības noteiktajām prasībām. Automatizēto risinājumu iestatījumi jāpārskata pēc nepieciešamības, bet ne retāk kā reizi gadā;

- *Žurnālfailu rotācija* – noteikt žurnālfailu dzēšanas un arhivēšanas politiku, kas nav pretrunā ar iekšējiem un ārējiem normatīvajiem aktiem.

5. ŽURNĀLFAILU PĀRVALDĪBAS POLITIKA

Organizācijām jāievieš žurnālfailu pārvaldības politika, kas ir atbilstoša organizācijas vajadzībām, darbības virzienam, saistošajiem normatīvajiem aktiem, labajām praksēm un auditu rezultātiem.

Žurnālfailu pārvaldības politikas kopumam jāsatur vismaz šādi punkti:

1. Lomu iedalījumu un atbildības līmeņus iesaistītajām personām un grupām (*piemēram, administratora, priviliģēta lietotāja, lietotāja un pārvaldnieka loma*);
2. Skaidri noteiktas obligātās un ieteicamās prasības žurnālfailu pārvaldībai (*piemēram, obligātās prasības, lai nodrošinātu žurnālfailu aizsardzību pret neautorizētu piekļuvi, ierakstu izmainīšanu un dzēšanu*);
3. Žurnālfailu pārvaldības politikas pārskatīšanas un izmaiņu kārtību (*piemēram, žurnālfailu pārvaldības politika tiek pārskatīta reizi gadā, un šajā procesā piedalās noteiktas personas*);
4. Prasības žurnālfailu uzglabāšanas un apstrādes infrastruktūrai un tās konfigurācijai (*piemēram, tiek centralizēti savākti un dublēti žurnālfaili uz citas infrastruktūras, šos resursus nodalot atsevišķā infrastruktūrā*);
5. Prasības žurnālfailu uzglabāšanas ilgumam, kas nav pretrunā ar MK Nr.397 57.punktā noteikto, kur tiek noteikts, ka žurnālfailus uzglabā:
    a) A klases informācijas sistēmām un to darbību nodrošinošām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām – vismaz 18 mēnešus pēc ieraksta izdarīšanas;
    b) B klases informācijas sistēmām un to darbību nodrošinošām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām – vismaz 12 mēnešus pēc ieraksta izdarīšanas;
    c) C klases informācijas sistēmām un to darbību nodrošinošām operētājsistēmām, pakalpēm (servisiem), tīklu un serveru iekārtām – vismaz 6 mēnešus pēc ieraksta izdarīšanas.

    Organizācija var izstrādāt arī detalizētāku žurnālfailu uzglabāšanas ilguma politiku, kas nav pretrunā ar MK Nr.397 57.punktu, izdalot žurnālfailus noteiktās grupās ar tās specifiskiem uzglabāšanas termiņiem, kā, piemēram, C klases informācijas sistēmai:
    - *Sistēmu žurnālfailu* uzglabā 6 mēnešus pēc ieraksta izdarīšanas;
    - *Informācijas sistēmas žurnālfailus* uzglabā 6 mēnešus pēc ieraksta izdarīšanas;
    - *Tīkla žurnālfailus* uzglabā 9 mēnešus pēc ieraksta izdarīšanas;
    - *Drošības žurnālfailus* uzglabā 9 mēnešus pēc ieraksta izdarīšanas;
    - *Datu bāzes žurnālfailus* uzglabā 6 mēnešus pēc ieraksta izdarīšanas;
    - *Nozīmīgu incidentu žurnālfailus* uzglabā 24 mēnešus pēc ieraksta izdarīšanas.

6. NOTIKUMI, PAR KURIEM JĀVEIDO ŽURNĀLFAILI

Organizācijai nepieciešams nodrošināt žurnālfailu uzskaiti, drošību un monitoringu, tādā līmenī, kas ļauj identificēt, izmeklēt un novērst dažāda veida incidentus, kas vērsti pret to un tās IKT resursiem.

MK Nr.397 3.9.apakšsadaļā "Žurnālfailu pārvaldība" žurnālfaili tiek iedalīti divās grupās – Informācijas sistēmas (58.punkts) un Tīkla plūsmas (60.punkts) žurnālfaili, kuros minēts vispārīgs minimālais žurnālfailu veidošanas apjoms.

Organizācijai žurnālfailu detalizācijas pakāpes veidošana jābalsta uz riska analīzes vērtējumu, kur ir ņemti vērā dažāda veida faktori, kā:

- saistošie normatīvie akti;
- Informācijas sistēmas drošības klase;
- Informācijas sistēmas žurnālfailu veidošanas iespējas;
- saistīto resursu žurnālfailu veidošanas iespējas;
- u.t.t.

Atbilstoši riska analīzei organizācijai jānosaka piemērota žurnālfailu veidošanas detalizācijas pakāpe. Jāņem vērā, ka nav vēlama situācija, kurā žurnālfailu veidošana prasa lielākas finanses un tehniskos resursus nekā attiecīgās sistēmas funkcionēšana un tās primārās funkcijas nodrošināšana, izņemot noteiktus gadījumus, kurās šāda situācija ir sagaidāma, piemēram, paaugstinātas drošības sistēmās.

6.1. INFORMĀCIJAS SISTĒMAS ŽURNĀLFAILI

Informācijas sistēmas žurnālfaili satur informāciju par konkrētās informācijas sistēmas notikumiem, kā:

1. informācijas sistēmas ieslēgšanu un izslēgšanu;

Piemēram:

- *Datoru un serveru (tai skaitā mākonī) operētājsistēmas līmeņa sistēmas ieslēgšanās un izslēgšanās un tās pieraksti.*

2. kontu izveidi, grozīšanu vai dzēšanu, kontu piekļuves tiesību izmaiņām;

Piemēram:

- *Datoru un serveru (tai skaitā mākonī) tiesību paaugstināšanu – dažādu lietotāju grupu un lietotāju profilu tiesību līmeņa paaugstināšana;*
- *Programmnodrošinājuma un informācijas sistēmu kontu:*
  - *izveidi, izmaiņām tajos vai dzēšanu;*
  - *tiesību paaugstināšanu – dažādu lietotāju grupu un lietotāju profilu tiesību līmeņa paaugstināšana.*

3. kontu piekļuvi informācijas resursiem, tostarp neveiksmīgiem piekļuves mēģinājumiem;

Piemēram:

- *Datoru un serveru (tai skaitā mākonī), komutatoru un maršrutētāju autentifikāciju – pieteikšanās (sekmīga un nesekmīga) un izlogošanās notikumi;*
- *Programmnodrošinājuma un informācijas sistēmu kontu:*

    - *autentifikāciju – pieteikšanās (veiksmīgi un nesekmīgi) un izlogošanās, izmaiņas autentifikācijas politikā un priviliģētu lietotāju/profilu/botu piekļuvē;*
    - *sesiju – informāciju par lietotāja sesijas darbībām, piemēram, pieslēgšanās un atslēgšanās, IP adresi un nozīmīgajām/būtiskajām sesijā veiktajām darbībām.*
- *Datu bāzes:*
    - *piekļuves pieprasījumi, tai skaitā žurnālfailos;*
    - *audita ieraksti – informācijas sistēmas iestatījumu, lietotāja tiesību un citu būtisku operāciju izmaiņu uzskaite.*
- *Video, IoT, u.t.t.:*
    - *piekļuvi iekārtai ar administrēšanas kontu, IP adresi, parametrizācijas izmaiņas un citus stāvokļus, ja tas ir iespējams.*

4. datu pievienošanu, izmaiņām, dzēšanu un datu atlasi;

Piemēram:

- *Programmnodrošinājuma un informācijas sistēmu notikumiem par svarīgajiem failiem – informācija par failu izveidi, modificēšanu, piekļuvi un dzēšanu (piemēram, informācijas sistēmas konfigurācijas izmaiņām).*

5. tehnisko resursu konfigurāciju izmaiņām;

Piemēram:

- *Datoru un serveru (tai skaitā mākonī) uzdevumu plānotājam (Task Scheduler, Cron job, Systemd Timers, u.c.) – jaunu un ieplānoto servisu un uzdevumu izveidēm un modificēšanu;*
- *Komutatoru un maršrutētāju konfigurācijas izmaiņas;*
- *Video, IoT, u.t.t. konfigurācijas izmaiņas, ja tas ir iespējams.*

6. informācijas sistēmas paziņojumiem, brīdinājumiem un citiem IKT notikumiem, kas varētu liecināt par kiberincidentu vai citu apdraudējumu informācijas sistēmas vai informācijas resursa drošībai.

Piemēram:

- *Datoru un serveru (tai skaitā mākonī):*
    - *operētājsistēmas līmeņa notikumiem – piemēram, procesu notikumiem (procesa nosaukumi, procesa ID, izpildes laiki un komandrindas argumenti, un operētājsistēmas reģistra izmaiņas);*
    - *kaitniecisku un ļaunprātīgu programmatūru atklāšana – paziņojumi no drošības risinājumu programmatūras (antivīrusu, XDR, ugunsmūris, u.c.);*
    - *notikumiem par svarīgajiem failiem – informācija par failu izveidi, modificēšanu, piekļuvi un dzēšanu (piemēram, sistēmas konfigurācijas izmaiņām).*
- *Programmnodrošinājuma un informācijas sistēmu pamatdarbību attēlojošie žurnālfaili – piemēram, Web serveru žurnālfailus, izvērtējot detalizācijas pakāpi atbilstoši spējai nodrošināt atbilstošu uzglabāšanas ilgumu;*

- *Komutatoru un maršrutētāju DHCP/Radius serveru izsniegtajām IP adresēm – kas satur informāciju par klienta iekārtas identifikatoru un IP adreses izmantošanas periodu;*
- *Datu bāzes citiem ierakstiem, kas identificēti kā organizācijai un to procesiem kritiskas darbības, piemēram, vaicājumi vai izmaiņu pieraksti.*

6.2. TĪKLA PLŪSMAS ŽURNĀLFAILI

Tīkla plūsmas žurnālfaili satur informāciju par:

1. datu nosūtīšanas un saņemšanas notikumiem;
2. notikuma laiku, kas sinhronizēts ar augstas precizitātes tīkla laika protokola (NTP) serveri (ntp.cert.lv), savukārt ja tehniski to nav iespējams nodrošināt, tad laika fiksēšanas metodi saskaņo ar Nacionālo kiberdrošības centru vai Satversmes aizsardzības biroju;
3. datu nosūtītāja (avota) un saņēmēja (galamērķa) IP;
4. izmantoto tīkla protokolu (piemēram, TCP, UDP);
5. avota un galamērķa izmantotos tīkla aplikācijas līmeņa protokolus (piemēram, HTTP, HTTPS, FTP);
6. ja attiecināms, avota unikālo identifikatoru (MAC adrese);
7. pārsūtīto (pārraidīto) datu apjomu.

6.3. VPN IEKĀRTU ŽURNĀLFAILI

Balstoties uz pieredzi un kiberincidentu analīzēm, atsevišķi jāizdala VPN žurnālfailu veidošanas nosacījumu minimālais apjoms, kas var būtiski atvieglot kiberincidentu izmeklēšanas procesu.

VPN iekārtu žurnālfailus veido par:

1. VPN – *Sekmīgos un nesekmīgos VPN autentifikācijas mēģinājumus, lietotāju sesijām piešķirtās IP adreses, VPN klienta iekārtas identificējošos parametrus (IP adrese, Hostname, OS, VPN programmatūras versijas dati) un izmantoto lietotāja autentifikācijas metodi;*
2. Caur VPN veikto datu plūsmas izlases metodes (*sampled netflow*) informācijas uzskaiti – *ienākošās un izejošās plūsmas avota un galamērķa IP adreses, portus, protokolus un savienojuma stāvokļus, piemēram, lietojot: NetFlow/sFlow;*

7. ŽURNĀLFAILU AIZSARDZĪBA UN ŠIFRĒŠANA

Žurnālfaili var saturēt ierobežotas pieejamības informāciju, līdz ar to, tie ir jāaizsargā pret neautorizētu piekļuvi, izmaiņām tajos vai dzēšanu to uzglabāšanas, apstrādes vai pārsūtīšanas procesā. Tādēļ organizācijām ir jāspēj nodrošināt vismaz:

1) Piekļuves kontrole žurnālfailiem – *tikai autorizētām personām, kuru piekļuve tiek fiksēta, un to pārvalda cita persona, nodrošinot vairāku acu principu (jāņem vērā, lai žurnālfaili nesatur autentifikācijas līdzekļu informāciju atklātā veidā, piemēram, lietotājvārda paroli, API key u.t.t.);*

2) Žurnālfailu šifrēšana – *lai samazinātu neautorizētu datu noplūdi informācijas pārsūtīšanā un uzglabāšanā, nepieciešams izmantot uzticamas šifrēšanas metodes, kā, piemēram, TLS 1.3 un AES-256;*
3) Integritātes nodrošināšana – *žurnālfailiem jānodrošina jaucējsummas pārvaldība, kas ietver tās pārbaudi, lai pārliecinātos par datu nemainīgumu. Jaucējsumma jāuzglabā atbilstoši drošības prasībām, lai nodrošinātu tās integritāti, un tā jāveido, izmantojot drošu algoritmu, piemēram, SHA-256.*

8. ŽURNĀLFAILU REZERVES KOPIJU PĀRVALDĪBA

Lai nodrošinātu žurnālfailu pieejamību arī informācijas sistēmu atteices, kiberdrošības incidentu vai citu ārkārtas gadījumu laikā, organizācijai ir jāievieš efektīva žurnālfailu rezerves kopiju pārvaldības kārtība.

Žurnālfailu rezerves kopiju pārvaldības mērķis ir novērst to zaudēšanu vai neatgriezenisku bojājumu, kas varētu būtiski apgrūtināt incidentu izmeklēšanu, drošības analīzi vai normatīvo prasību izpildi. Žurnālfailu rezerves kopiju pārvaldībā ieteicams ievērot sekojošo:

1) Rezerves kopiju veidošana – *atbilstoši organizācijā noteiktajiem kritērijiem veidot regulāras un automātiskas kritisko žurnālfailu rezerves kopijas drošā infrastruktūrā, piemēram, eksportējot un noteiktu laiku periodu uzglabājot ārējā ar tīklu nesaistītā infrastruktūrā;*
2) Uzglabāšana citā lokācijā – *rezerves kopijas uzglabāšana citā fiziskā lokācijā vai mākonī ar mērķi nodrošināt aizsardzību pret datu zaudēšanu dabas katastrofā vai kiberuzbrukuma rezultātā;*
3) Rezerves kopiju uzglabāšanas termiņš – *atbilstoši organizācijas vajadzībām, bet ne mazāk kā tās noteikts MK Nr.397 57.punktā* (*A drošības klases sistēmai 18 mēnešus pēc ieraksta izdarīšanas, B klases sistēmai 12 mēnešus un C klases sistēmai 6 mēnešus*);
4) Rezerves kopiju uzglabāšanas vieta – *žurnālfailus jāuzglabā nodalīti no attiecīgās sistēmas, tīkla vai IKT infrastruktūras.*

9. REĀLLAIKA MONITORINGS UN IZMEKLĒŠANA

Žurnālfaili ieņem būtisku lomu incidentu identificēšanā, reaģēšanā un izmeklēšanā. Lai savlaicīgi atklātu iespējamos apdraudējumus un mazinātu to ietekmi, organizācijai jānodrošina efektīvi mehānismi žurnālfailu analīzei, tai skaitā reāllaika monitoringam.

1) Žurnālfailu reāllaika uzraudzība – *automatizētas sistēmas, kas reāllaikā balstoties uz saņemtajiem datiem spēj atklāt incidentus un reaģēt uz tiem;*
2) Žurnālfailu uzglabāšana kiberincidenta izmeklēšanai – *notiekot kiberincidentam, nepieciešams saglabāt visus iesaistītos žurnālfailus kā arī nodrošināt to aizsardzību pret manipulācijām;*
3) Uzraudzības ķēde *(Chain of Custody) – nepieciešams dokumentēt un uzturēt skaidru žurnālfailu pārvaldības ķēdi un nodrošināt izmeklēšanu atbilstoši organizācijā noteiktajām prasībām.*

CERT.LV nodrošina Drošības operācijas centra (SOC) pakalpojumu kritiskās infrastruktūras, valsts un pašvaldību iestādēm, reālā laikā uzraugot drošības telemetriju (tai skaitā žurnālfailu analīzi), lai savlaicīgu pamanītu kiberapdraudējumus, kiberincidentus un mazinātu to kaitējumu. Žurnālfaili tiek uzglabāti ne vairāk kā 6 mēnešus.

10.ŽURNĀLFAILU ARHIVĒŠANA

Ilgtermiņa uzglabāšanai paredzētie žurnālfaili, kuri vairs netiek aktīvi izmantoti, bet joprojām ir jāsaglabā organizācijas interesēs, vai pēc normatīvo aktu vai standartu prasībām, ir jāarhivē.

1) Aukstā uzglabāšana *(Cold Storage) – arhivētie žurnālfaili ir jāpārvieto uz auksto uzglabāšanu, lai samazinātu uzglabāšanas izmaksas, bet tajā pašā laikā jānodrošina atbilstība žurnālfailu uzglabāšanas prasībām;*

2) Žurnālfailu ilgtermiņa apstrādes datu formāts – *par žurnālfailiem atbildīgajai personai jānosaka uzglabāšanas datu formāts (Syslog, JSON, XML, u.c.), tiem jābūt nolasāmiem un izmantojamiem pēc vairākiem gadiem;*

3) Žurnālfailu uzglabāšanas veids – *par žurnālfailiem atbildīgajai personai jāparedz atbilstošs uzglabāšanas veids (CDs, DVDs, NAS, SAN, u.t.t.), kas būs izmantojams un apstrādājams pēc noteikta perioda;*

4) Integritātes pārbaude – *veicot žurnālfailu pārvietošanu, nepieciešams nodrošināt jaucējsummas izveidi un uzglabāšanu drošā veidā, lai nodrošinātu datu integritāti pārvietošanas un uzglabāšanas procesā;*

5) Fiziskā drošība – *jānodrošina atbilstoša fiziskā un loģiskā drošība tehniskajiem resursiem, kuros uzglabā žurnālfailus, kas ietver piekļuves kontroli, mitruma un temperatūras monitorēšanu, kā arī citas darbības, lai nodrošinātu žurnālfailu drošību;*

6) Piekļuve arhīviem – *tikai pilnvarotas personas var piekļūt uzglabātajam arhīvam, ievērojot žurnālfailu piekļuves prasības, piemēram, kurš un kāpēc ir piekļuvis un kādas darbības ir veicis.*