*Nacionālais kiberdrošības centrs, 29.07.2025.*

**[NKDL Subjekta indentificējoša informācija]**

**Kiberincidentu pārvaldības kārtība un kiberincidentu žurnāls**

*Procedūras kiberincidentu identificēšanai, reģistrēšanai, novēršanai un ziņošanai, kā arī žurnāls incidentu uzskaitei (žurnalēšana var būt digitāla).*

|  |  |  |
| --- | --- | --- |
| Nr. | Apakšnodaļa nosaukums | Statuss |
| 1. | Ievads | ✔️ Obligāta |
| 2. | Reaģēšanas posmi | ✔️ Obligāta |
| 3. | Incidentu klasifikācija | ✔️ Obligāta |
| 4. | Incidentu reģistrs (žurnāls) | ✔️ Obligāta |
| 5. | Ziņošana iestādēm | ✔️ Obligāta |
| 6. | Pārskatīšana un uzlabošana | ✔️ Obligāta |

**Saturs**

[1. Ievads 3](#_Toc204684221)

[2. Reaģēšanas posmi 3](#_Toc204684222)

[3. Incidentu klasifikācija 5](#_Toc204684223)

[4. Incidentu žurnāls 6](#_Toc204684224)

[5. Komunikācija 7](#_Toc204684225)

[5. Ziņošana iestādēm 7](#_Toc204684226)

[6. Pārskatīšana un uzlabošana 7](#_Toc204684227)

# 1. Ievads

Kiberincidentu pārvaldības kārtības mērķis ir definēt organizācijas gatavību atklāt, reaģēt, ierobežot un atgūties no kiberdrošības incidentiem, gandrīz notikušiem kiberincidentiem un ievainojamībām.

Nepieciešams noteikt:

* Kārtību, kā tiek identificēti kiberincidenti, gandrīz notikuši kiberincidenti un ievainojamības, t.sk., iegūstot informāciju no darbiniekiem, ārpakalpojumu sniedzējiem, trešajām personām.
* Principus, kā tiek pārvaldīta pieeja žurnālfailiem (autentifikācija, saglabāšana, dzēšana).
* Iekļaut norādi par testēšanas biežumu un treniņu scenārijiem incidentu pārvaldībā.
* Komunikācijas kārtību. Par kiberincidentu nekavējoties jāinformē CERT.LV. Nozīmīgu kiberincidentu gadījumā jāziņo CERT.LV, iesniedzot agrīno brīdinājumu, sākotnējo ziņojumu, gala ziņojumu, progresa ziņojumu un starpposma ziņojumu, izmantojot [25.06.2025. MK noteikumos Nr. 397](https://likumi.lv/ta/id/361481-minimalas-kiberdrosibas-prasibas) pielikumos iekļautās ziņojumu formas.
* Saziņu incidenta gadījumā jāveic caur definētiem kontaktpersonu kanāliem. Iekļauj norādi par iekšējiem ziņošanas kanāliem, kam darbiniekiem jāziņo, u.tml.
* Iesaistīto personu lomu un atbildības sadalījums kiberincidenta pazīmju konstatēšanas gadījumā vai informācijas saņemšanas gadījumā par iespējamo vai gandrīz notikušu kiberincidentu.

# 2. Reaģēšanas posmi

Tiek noteikti procesi katram reaģēšanas posmam:

1. Identifikācija – tiek atklāts potenciāls incidents (SIEM, IDS, SOC ziņojumi).
2. Apstiprināšana un klasifikācija – tiek izvērtēts incidents, tā nopietnība un ietekme.
3. Eskalācija – informācija nodota atbildīgajai komandai un vadībai.
4. Risināšana – tiek veikti pasākumi incidenta neitralizēšanai un ietekmes mazināšanai.
5. Atjaunošana – pakalpojumu un sistēmu atjaunošana.
6. Mācības – pēc-incidenta analīze (*post-incident review*), korekcijas kontroles pasākumos un procedūrās.

|  |  |  |
| --- | --- | --- |
| Datu lauks | MK pants | Paskaidrojums |
| Incidenta konstatēšanas datums un laiks | 48.1. | Kad incidents tika konstatēts. |
| Incidenta notikšanas datums un laiks | 48.1. | Kad incidents reāli notika (ja zināms). |
| Veida kods | 48.2. | Saskaņā ar 7. pielikuma tipoloģiju. |
| Vispārīgs apraksts | 48.3. | Īss apraksts par incidentu. |
| Cēloņi un kompromitēšanas indikatori | 48.4. | Kas izraisīja incidentu, kā tas tika atklāts (logi, rīki utt.). |
| Ietekmes novērtējums | 48.5. | Zema, Vidēja, Augsta u.tml. |
| Nozīmīguma atzīme | 48.6. | Vai tas klasificējas kā nozīmīgs incidents. |
| Ziņošanas statuss | 48.7. | Vai un kādi ziņojumi iesniegti CERT.LV: agrīnais, sākotnējais u.c. |
| Risināšanas statuss | 48.8. | Neiesākts, Procesā, Atrisināts. |

Organizācija uztur kiberincidentu žurnālu, kurā reģistrē ziņas par konstatētajiem kiberincidentiem:

* Reģistrē incidentu ne vēlāk kā **24 stundu laikā** no konstatēšanas.
* Aktualizē žurnālu pēc jebkādām izmaiņām iepriekš žurnālā norādītajās ziņās ne vēlāk kā 24 stundu laikā.
* Žurnālā jāiekļauj vismaz:
	+ Konstatēšanas datums/laiks;
	+ Kiberincidenta datums un laiks, ja zināms;
	+ Kiberincidenta veida kods atbilstoši 25.06.2025.MK noteikumiem Nr. 397kas minēti arī šīs kārtības 3. apakšnodaļā;
	+ Kiberincidenta apraksts, cēloņi un kompromitēšanas indikatori, ietekmes novērtējums;
	+ Atzīme, vai kiberincidents ir nozīmīgs;
	+ Ziņošanas statuss CERT.LV;
	+ Incidenta statuss (piem.: "procesā", "atrisināts").
* Incidentu pārvaldības plāns jāpārskata **reizi gadā** vai **pēc augstas ietekmes incidenta**.
* Pēc incidentu analīze jāizmanto **kontroles un apmācību uzlabošanai**.
* Jādokumentē veiktie uzlabojumi un jāveic audits vai pašvērtējums.

# 3. Incidentu klasifikācija

Incidents tiek klasificēts pēc tā veida (ļaunprogrammatūra, iekšējs pārkāpums, DDoS, nesankcionēta piekļuve) un ietekmes (zema, vidēja, augsta).

Lai incidentu klasifikācija pilnībā **atbilstu** **26.06.2025. MK noteikumu Nr. 397 prasībām**, tai ir jābalstās uz:

1. **kiberincidentu tipoloģiju (veida klasifikācija), atbilstoši** [MK noteikumu 7. pielikumam.](https://likumi.lv/ta/id/361481-minimalas-kiberdrosibas-prasibas%22%20%5Cl%20%22piel7)
2. **ietekmes novērtējumu.**
3. **nozīmīguma novērtējumu, atbilstoši** [26.06.2025. MK noteikumu Nr. 397 7. nodaļai “Kiberincidentu vadība”](https://likumi.lv/ta/id/361481#p117)**.**

Kiberincidentu tipoloģija

|  |  |
| --- | --- |
| Kods | Kiberincidenta vai gandrīz notikuša kiberincidenta veids |
| 01 | Neatbilstošs saturs (piemēram, mēstule, nelegāls saturs) |
| 02 | Ļaundabīgs kods |
| 03 | Informācijas vākšana |
| 04 | Ielaušanās mēģinājums |
| 05 | Ielaušanās |
| 06 | Pieejamības traucējums |
| 07 | Datu drošības pārkāpums (piemēram, nesankcionēta piekļuve vai modificēšana) |
| 08 | Krāpniecība |
| 09 | Ievainojamība |
| 10 | Cits kiberincidenta veids |
| 99 | Pārbaude (mācības) |

# 4. Incidentu žurnāls

Zemāk žurnāla piemērs:

|  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Incidenta notikšanas datums | Kiberincidenta konstatēšanas datums un laiks | Veids (7. pielikums) | Vispārīgs apraksts | Cēloņi / indikatoru piemēri | Ietekmes novērtējums | Nozīmīgs? (Jā/Nē) | Ziņots CERT (atzīmes) | Statuss (neiesākts / procesā / atrisināts) | Atbildīgais |
| 1 | 2025-03-01 |  | 01 | Viltots e-pasts ar ļaunatūru pielikumā | Sūtītājs no ārēja domēna, aizdomīgs URL | Vidēja | Nē | - | Atrisināts | Drošības analītiķis |
| 2 | 2025-03-02 |  | 07 | FTP ievainojamība izmantota piekļuvei | Ievainojams ports, netipiski savienojumi | Augsta | Jā | Agrīnais, Sākotnējais, Gala ziņojums | Atrisināts | Kiberdrošības pārvaldnieks |

# 5. Komunikācija

Iekšējās un ārējās komunikācijas plāns. Informācija par to, kam darbinieki pakalpojumu sniedzēji ziņo par konstatētiem kiberincidentiem, gandrīz notikušiem kiberincidentiem, ievainojamībām.

Plāns ietver informāciju, kādas personas tiek iesaistītas kiberincidenta risināšanā, to pienākumu uzskaitījumu un atbildības jomas.

Plāns ietver informāciju, kā tiek veikta iekšējā un uz āru veiktā saziņa, t.sk., vai un kādos gadījumos tiek informēti subjekti, sabiedrība, kad tiek informēti sadarbības partneri, u.tml.

# 5. Ziņošana iestādēm

Konstatējot kiberincidentu, par to nekavējoties informē kiberincidentu novēršanas institūciju (CERT.LV), nosūtot uz tās elektroniskā e-pasta adresi kiberincidenta aprakstu brīvā formā. Aprakstā var iekļaut informāciju, kas par attiecīgo kiberincidentu tiek reģistrēta kiberincidentu žurnālā.

Nozīmīgi kiberincidenti jāziņo CERT.LV nekavējoties, bet ne vēlāk kā 24 stundu laikā no to konstatēšanas brīža, iesniedzot agrīno brīdinājumu par nozīmīgu kiberincidentu.

Atbilstoši un ievērojot Nacionālās kiberdrošības likuma 34. pantā noteiktos termiņus, CERT.LV tiek informēts par kiberincidentu un tā risināšanas progresu, izmantojot šādas ziņojumu formas, kas pieejamas [25.06.2025. MK noteikumu Nr. 397](https://likumi.lv/ta/id/361481%22%20%5Cl%20%22piel10) **pielikumos**:

* + Agrīnais brīdinājums;
	+ Sākotnējais ziņojums;
	+ Progresa ziņojums;
	+ Starpposma ziņojums;
	+ Gala ziņojums.

Jāizmanto iepriekš definēti saziņas kanāli un kontaktpersonu saraksts (organizācijā jābūt noteiktiem atbildīgajiem par ziņošanu). Ziņojumus var sūtīt šifrētā formātā. Nozīmīgu kiberincidentu gadījumā elektroniski jāaizpilda [25.06.2025. MK noteikumu Nr. 397](https://likumi.lv/ta/id/361481) noteiktās ziņojumu formas, tās jāparaksta ar drošu elektronisko parakstu un jānosūta CERT.LV uz tās elektronisko e-pasta adresi.

Var norādīt informāciju par ziņošanas iespēju Valsts policijai.

Var norādīt informāciju par ziņošanu Datu valsts inspekcijai, ja kiberincidentā ir ietekmēti personas dati.

# 6. Pārskatīšana un uzlabošana

Incidentu pārvaldības plāns tiek pārskatīts reizi gadā vai pēc katra augsta ietekmes incidenta.

Pēc-analīzes rezultāti tiek izmantoti kontroles pasākumu un apmācību uzlabošanai.