*Nacionālais kiberdrošības centrs*, *29.07.2025.*

**[NKDL Subjekta indentificējoša informācija]**

**Kiberrisku pārvaldības
un IKT darbības nepārtrauktības plāns**

*Plāns, kas ietver risku identifikāciju, novērtējumu, pārvaldības pasākumus un darbības nepārtrauktības nodrošināšanu*

|  |  |  |
| --- | --- | --- |
| Nr. | Apakšnodaļa nosaukums | Statuss |
| 1. | Vispārīga informācija | ✔️ Obligāta |
| 2.1 | Riska novērtēšanas metodoloģija | ✔️ Obligāta |
| 2.2 | Riska identificēšana | ✔️ Obligāta |
| 2.3 | Riska analīze un novērtējums | ✔️ Obligāta |
| 3.1 | Riska novērtēšanas process | ✔️ Obligāta |
| 4.1 | Riska apstrāde | ✔️ Obligāta |
| 5. | Incidentu pārvaldība | ✔️ Obligāta |
| 6. | Kontroles un uzraudzības mehānismi | ✔️ Obligāta |
| 7. | Secinājumi un ieteikumi | ☑ Rekomendējama |
| 8. | Nepārtrauktības plāns (BCP) | ✔️ Obligāta |
| 9. | Pārskatīšana un testēšana | ✔️ Obligāta |

**SATURS**

[1. VISPĀRĪGĀ INFORMĀCIJA 3](#_Toc204683841)

[2. RISKA NOVĒRTĒŠNAS METoDoLOĢIJA 4](#_Toc204683842)

[2.1. Riska novērtēšanas metodoloģija 4](#_Toc204683843)

[2.2. Riska identificēšana 4](#_Toc204683844)

[2.3. Riska analīze un novērtējums 4](#_Toc204683845)

[3. RISKA NOVĒRTĒJUMS UN ANALĪZE 5](#_Toc204683846)

[3.1. Riska novērtēšanas process 5](#_Toc204683847)

[4. RISKA PĀRVALDĪBAS PASĀKUMI 7](#_Toc204683848)

[4.1. Riska apstrāde 7](#_Toc204683849)

[4.2. Incidentu pārvaldības procesi 7](#_Toc204683850)

[5. KONTROLES UN UZRAUDZĪBAS PROCESI 9](#_Toc204683851)

[6. SECINĀJUMI UN IETEIKUMI 9](#_Toc204683852)

[7. NEPĀRTRAUKTĪBAS PLĀNS (BCP) 9](#_Toc204683853)

[8. PĀRSKATĪŠANA UN TESTĒŠANA 9](#_Toc204683854)

# VISPĀRĪGĀ INFORMĀCIJA

**Organizācijas struktūra:** detalizēts pārvaldītāja struktūras un atbildību apraksts.

Šajā sadaļā jānorāda:

* Struktūrvienības vai amatpersonas, kas atbildīgas par kiberdrošību;
* Lomu un atbildību sadalījums (piem., IT vadītājs, incidentu reģistrētājs, pārvaldnieks);
* Atbildīgo personu(-as) par kiberrisku pārvaldības un IKT darbības nepārtrauktības plāna izstrādi, pārskatīšanu un aktualizēšanu, kā arī par plānā ietverto pasākumu īstenošanu;
* Kā tiek nodrošināta sadarbība ar ārējām iestādēm (piem., CERT.LV).

**Tehniskā infrastruktūra:** pārskats par izmantotajām tehnoloģijām un sistēmām.

Organizācijai jāuztur aktuāls pārskats par:

* IKT resursiem (serveri, darbstacijas, tīkla iekārtas, datu nesēji u.c.);
* Informācijas sistēmām un lietojumprogrammām (piem., grāmatvedības, e-pasta, klientu apkalpošanas sistēmas);
* To uzturēšanas modeli – iekšēja vai ārpakalpojums;
* Norādīt fizisko un virtuālo izvietojumu, kā arī atbildīgos.

**Pakalpojumu sniegšana:** apraksts par piedāvātajiem pakalpojumiem un to nozīmi.

Aprakstīt nozīmīgos kritērijus:

* Aprakstīt organizācijas **piedāvātos pakalpojumus**, kas saistīti ar informācijas sistēmām;
* Norādīt, kuri no tiem ir **būtiski vai svarīgi pakalpojumi** (piem., maksājumu apstrāde, datu piekļuves portāli);
* Izskaidrot šo pakalpojumu **lomu un ietekmi**, ja tie kļūtu nepieejami (iestātos kiberdrošības incidents).

# RISKA NOVĒRTĒŠNAS METoDoLOĢIJA

## Riska novērtēšanas metodoloģija

 Pielietotās metodes: kvalitatīva un kvantitatīva novērtēšana;

 Datu vākšanas un apstrādes avoti (logi, incidenti, darbinieku intervijas u.c.).

## Riska identificēšana

Klasifikācija pēc risku izcelsmes:

* Fiziskie riski
* Personāla riski
* Tehniskie riski
* Programmatūras riski
* Dabas un vides riski
* Trešo pušu riski

##  Riska analīze un novērtējums



Attēls 1. Riska vērtību matricas piemērs

**Risku tabula ar klasifikāciju pēc:**

* Iespējamības (1–5)
* Ietekmes (1–5)
* **Riska līmenis** = Iespējamība × Ietekme

Tabula 1. Riska novērtēšanas un pārvaldības piemērs

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| **ID** | **Riska apraksts** | **Iespējamība** | **Ietekme** | **Riska līmenis** | **Kontrole** | **Atbildīgais** | **Piezīmes** |
| 1.1 | Fiziskās drošības pārkāpums | .. | .. | .. | … | Kiberdrošības Pārvaldnieks | – |
| ... | ... | ... | ... | ... | ... | ... | ... |

# RISKA NOVĒRTĒJUMS UN ANALĪZE

##  Riska novērtēšanas process

Riski tiek noteikti, ņemot vērā trīs komponentes: draudus, ievainojamības un iespējamo ietekmi uz aktīvu. Katram identificētajam riskam tiek piešķirts riska līmenis, kas tiek noteikts pēc kombinētās vērtības skalas.

Riska vērtēšana tiek veikta ar šādiem soļiem:

1. Kiberriskam pakļauto IKT resursu identificēšana un vērtēšana.
2. Apdraudējumu un ievainojamību identificēšana.
3. Riska līmeņa aprēķināšana (Ietekme × Varbūtība).
4. Riska pārvaldības metodes izvēle (izvairīšanās, pārnešana, pieņemšana, pārvaldīšana.



Attēls 2. Riska novērtēšanas procesa un apstrādes plāna piemērs

Veicot atkārtotu risku analīzi, ir [jāveic salīdzinājums](https://likumi.lv/ta/id/361481#p41)  ar iepriekšējā periodā veikto kiberrisku analīzi.

Tabula 2. Risku kontroles un pārvaldības piemērs.

|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ID / NR. | RISKA APRASTS | IESPĒJAMĪBA1 – 5 | IETEKME1 – 5 | VĒRTĪBAiesp. x ietekme | KONTROLENepārtrauktības plāns | ATBILDĪGIE | PIEZĪMES(piem., kontroles īstenošanas termiņš vai tā periodiskums) |
| 1. AR FIZISKO DROŠĪBU SAISTĪTIE RISKI
 |
| 1.1. |   |  |  |  |   |   |   |
| 1.2. |   |  |  |  |   |   |   |
| 1. AR PERSONĀLU SAISTĪTI RISKI
 |
| 2.1. |   |  |  |  |   |   |   |
| 2.2. |   |  |  |  |   |   |   |
| 1. AR TEHNIKU SAISTĪTIE RISKI
 |
| 3.1. |   |  |  |  |   |   |   |
| 3.2. |   |  |  |  |   |   |   |
| 1. AR PROGRAMMATŪRU SAISTĪTIE RISKI
 |
| 4.1. |   |  |  |  |   |   |   |
| 4.2. |   |  |  |  |   |   |   |
| 1. AR DABU UN VIDI SAISTĪTIE RISKI
 |
| 5.1. |   |  |  |  |   |   |   |
| 5.2. |   |  |  |  |   |   |   |
| 1. AR TREŠAJĀM PUSĒM SAISTĪTIE RISKI
 |
| 6.1. |   |  |  |  |   |   |   |
| 6.2. |   |  |  |  |   |   |   |

# RISKA PĀRVALDĪBAS PASĀKUMI

##  Riska apstrāde

Piemēram:

* Preventīvie pasākumi: piekļuves kontrole, ugunsmūri, rezerves kopijas;
* Identificēšanas pasākumi: SIEM sistēmas, žurnālu analīze;
* Korektīvie pasākumi: incidentu atbildes plāni, procedūru pārskatīšana.

Tabula 3. Riska kontroles veidu aprakstošs piemērs

|  |  |
| --- | --- |
| Kontroles veids | Funkcija |
| Preventīvās | Novērst apdraudējumus pirms to iestāšanās |
| Korektīvās | Atjaunot sistēmu darbību pēc incidenta |
| Detektīvās (identificējošās) | Atklāt un identificēt drošības notikumus |
| Atturošās (izolējošās) | Samazināt apdraudējuma iespējamību ar psiholoģisku vai vizuālu efektu |
| Administratīvās (uzturēšana un atjaunošana) | Noteikt rīcību, atbildības, lēmumu pieņemšanas kārtību |

##  Incidentu pārvaldības procesi

Tabula 4. Incidentu pārvaldības piemērs

|  |  |
| --- | --- |
| PĀRVALDI | Organizācijas konteksts |
| Riska pārvaldības stratēģija |
| Lomas, atbildības un autoritātes |
| Politikas |
| Pārraudzība |
| Kiberdrošības piegādes ķēde un riska pārvaldība |
| **IDENTIFICĒ** | Aktīvu pārvaldība |
| Riska vērtēšana |
| Uzlabošana |
| **AIZSARGĀ** | Identitātes pārvaldība, autentifikācija un piekļuves kontrole |
| Informētība un apmācības |
| Datu drošība |
| Platformas drošība |
| Tehnoloģiju infrastruktūras noturība |
| **ATKLĀJ** | Nepatraukta uzraudzība |
| Nevēlamo notikumu analīze |
| **REAĢĒ** | Incidentu pārvaldība |
| Incidentu analīze |
| Incidentu reaģēšanas ziņošana un komunikācija |
| Incidentu vadība (izolēšana un izskaušana) |
| **ATJAUNO** | Incidentu atveseļošanās plāns  |
| Incidentu atjaunošanās komunikācija |

Tabula 5. Kiberincidentu tipoloģija atbilstoši [MK noteikumu “Minimālās kiberdrošības prasības” 7. pielikumam](https://likumi.lv/ta/id/361481#p48)

|  |  |
| --- | --- |
| Kods | 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) |

# KONTROLES UN UZRAUDZĪBAS PROCESI

* Drošības auditi un ievainojamību skenēšana.
* KPI sistēmas efektivitātes uzraudzībai.
* Riska novērtējuma periodiska atjaunošana (vismaz reizi gadā vai pēc būtiskām izmaiņām).

# SECINĀJUMI UN IETEIKUMI

**Galvenie secinājumi:**
Kritiskākie identificētie riski, to ietekme un nepietiekami kontroles mehānismi.

**Plānotie uzlabojumi:**

* Riska apstrādes pasākumu paplašināšana;
* Darbinieku apmācības;
* Uzraudzības uzlabošana.

# NEPĀRTRAUKTĪBAS PLĀNS (BCP)

**Piezīme:** var būt atsevišķi.

Informācija par to, kā organizācijā tiek norosināta pakalpojumu nepārtrauktība, lai saglabātu konfidencialitāti, integritāti un pieejamību.

Nepārtrauktības plāna mērķis ir nodrošināt kritisko pakalpojumu sniegšanu, pat ja noticis kiberdrošības incidents, tehniska kļūme vai fiziska katastrofa. BCP balstās uz šādiem komponentiem (piemērs):

* + kritisko procesu saraksts;
	+ RTO/RPO/MTD noteikšana un to uzraudzības metodika;
	+ rīcības plāns, ja RTO/RPO/MTD tiek pārsniegts;
	+ avārijas kontaktpersonu saraksts;
	+ alternatīvas darba vietas un sistēmas;
	+ sakaru plāns iekšējai un ārējai informēšanai;
	+ atjaunošanas darbību plāns kiberincidenta vai krīzes gadījumā.

#  PĀRSKATĪŠANA UN TESTĒŠANA

Kiberrisku pārvaldības un nepārtrauktības plāns tiek pārskatīts un aktualizēts reizi gadā vai pēc būtiska incidenta. Plāna testēšana tiek veikta, izmantojot simulācijas, galda vingrinājumus un tehniskās atjaunošanas pārbaudes.