*Nacionālais kiberdrošības centrs, 29.07.2025.*

**[NKDL Subjekta indentificējoša informācija]**

**Kiberdrošības riskam pakļauto
IKT resursu un informācijas sistēmu katalogs**

*Saraksts ar visiem būtiskajiem kiberriskam pakļautajiem IKT resursiem.*

|  |  |  |
| --- | --- | --- |
| Nr. | Apakšnodaļa nosaukums | Statuss |
| 1. | Vispārīgā informācija | ✔️ Obligāta |
| 2. | IKT resursu pārvaldības principi | ☑ Rekomendējama |
| 3. | Resursu klasifikācija | ✔️ Obligāta |
| 4. | Resursu aizsardzības pasākumi | ✔️ Obligāta |
| 5. | Atbildības un uzturēšanas kārtība | ☑ Rekomendējama |
| 6. | Pielikumi (formas, kritēriji, saraksti) | ✔️ Obligāta |

SATURS

[VISPĀRĪGĀ INFORMĀCIJA 3](#_Toc204681016)

[IKT RESURSU PĀRVALDĪBAS PRINCIPI 3](#_Toc204681017)

[RESURSU KLASFIKĀCIJA 3](#_Toc204681018)

[RESURSU AIZSARDZĪBAS PASĀKUMI 3](#_Toc204681019)

[ATBILDĪBAS UN UZTURĒŠANSA KĀRTĪBA 3](#_Toc204681020)

[RISKAM PAKĻAUTIE IKT RESURSI 4](#_Toc204681021)

# VISPĀRĪGĀ INFORMĀCIJA

Katalogā ietverts visu būtisko IKT resursu saraksts ar:

* resursa veidu, nosaukumu un aprakstu,
* klasifikāciju (konfidencialitāte, pieejamība, integritāte, kritiskums),
* īpašnieku un atbildīgo pārvaldītāju.

**Terminu skaidrojums**

**IKT resurss** – jebkura informācijas apstrādes vai glabāšanas sistēma, programmatūra, datu kopums u.c.

**Kritiskais resurss** – resurss, kura nepieejamība būtiski ietekmē pakalpojumu sniegšanu.

**Resursu īpašnieks** –organizācijās īpašnieks tā deleģēta persona vai vienība, kas ir atbildīga par datu saturu un klasifikāciju.

**Klasifikācija** – resursa drošības klases līmenis atbilstoši konfidencialitātei, pieejamībai un integritātei.

## IKT RESURSU PĀRVALDĪBAS PRINCIPI

* **Inventarizācija** – regulāra resursu uzskaite un atjaunošana.
* **Klasifikācija** – pēc drošības klases un kritiskuma līmeņa.
* **Aizsardzība** – atbilstošu kontroles pasākumu piemērošana.
* **Atbildība** – lomu un pienākumu noteikšana katram resursam.

## RESURSU KLASFIKĀCIJA

* **Drošības klases līmeņi**: atbilstoši  [25.06.2025. MK noteikumos Nr. 397 noteiktajai metodikai](https://likumi.lv/ta/id/361481#p32).
* **Kritiskuma līmenis**: Augsts / Vidējs / Zems.
* **Riska faktori**: iespējamie apdraudējumi un ievainojamības.

## RESURSU AIZSARDZĪBAS PASĀKUMI

* **Piekļuves kontrole (**RBAC, MFA u.c.)
* **Monitorings un žurnālfaili**
* **Rezerves kopēšana un atjaunošana**
* **Atjaunošanas plāni (DRP/BCP)**

## ATBILDĪBAS UN UZTURĒŠANSA KĀRTĪBA

* Resursu īpašnieks – nosaka klasifikāciju un izmantošanas noteikumus.
* **IT atbalsts** – nodrošina tehnisko uzturēšanu.
* **Aktualizēšana** – vismaz reizi gadā vai izmaiņu gadījumā nekavējoties, bet ne vēlāk kā viena mēneša laikā.

# **RISKAM PAKĻAUTIE IKT RESURSI**

|  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Nr. | Resursa nosaukums | Resursa tips | Apraksts | Atrašanās vieta | Resursa īpašnieks | Kritiskums | Drošības klase | Pēdējā atjaunošana |
| 1 | Active Directory Server | Serveris | Lietotāju autentifikācija | Datu centrs Rīga | IT nodaļa | Augsts | A | 29/05/2025 |
| 2 | HR lietotne | Programma | Personāla datu pārvaldība | Iekšējais tīkls | HR nodaļa | Augsts | A | 29/05/2025 |
| 3 | VPN risinājums | Tīkla pakalpojums | Attālinātas piekļuves nodrošinājums | Mākoņpakalpojums | IT nodaļa | Videjs | B | 29/05/2025 |
| 4 | E-pasta serveris | Serveris | Iekšējā un ārējā komunikācija | Mākoņpakalpojums | IT nodaļa | Vidējs | B | 29/05/2025 |
| 5 | Komercnoslēpums |  |  |  |  |  | A |  |