*Nacionālais kiberdrošības centrs, 29.07.2025.*

**[NKDL Subjektu indentificējoša informācija]**

**Kiberdrošības procedūru politika**

*Noteikumi par iekšējām fiziskajām, loģiskajām un tehniskajām drošības kontrolēm informācijas sistēmas aizsardzībai*

|  |  |  |
| --- | --- | --- |
| Nr. | Apakšnodaļa nosaukums | Statuss |
| 4.1 | Informācijas sistēmas pārvaldība un politika | ✔️ Obligāta |
| 4.2 | Informācijas aktīvu pārvaldība | ✔️ Obligāta |
| 4.3 | Risku pārvaldība | ✔️ Obligāta |
| 4.4 | Fiziskā un vides drošība | ✔️ Obligāta |
| 4.5 | Piekļuves kontrole | ✔️ Obligāta |
| 4.6 | Cilvēkresursu drošība | ✔️ Obligāta |
| 4.7 | Apmācība un informētība | ✔️ Obligāta |
| 4.8 | Tīkla un darba staciju drošība | ✔️ Obligāta |
| 4.9 | Aplikāciju drošība | ☑ Rekomendējama |
| 4.10 | Konfigurācija pārvaldība | ☑ Rekomendējama |
| 4.11 | Incidentu apstrāde | ✔️ Obligāta |
| 4.12 | Nepārtrauktība un krīzes vadība | ✔️ Obligāta |
| 4.13 | Kriptogrāfija | ✔️ Obligāta |
| 4.14 | Atbilstības un piegāžu ķēžu drošība | ✔️ Obligāta |
| 4.15 | Uzraudzība, žurnālfaili un auditi | ✔️ Obligāta |
| 4.16 | Datu rezerves kopēšana un atjaunošana | ✔️ Obligāta |
| 4.17 | Iznīcināšana | ✔️ Obligāta |
| 4.18 | Uzlabošana un korektīvās darbības | ☑ Rekomendējama |
| 5. | Iekšējās kontroles un audita kārtība | ✔️ Obligāta |
| 6. | Ārpakalpojumu pārvaldība | ✔️ Obligāta |

**SATURS**

[VISPĀRĒJĀS PRASĪBAS 3](#_Toc204683172)

[1. INFORMĀCIJAS SISTĒMAS UN RISKU PĀRVALDĪBA 4](#_Toc204683173)

[2. PLĀNOŠANA 4](#_Toc204683174)

[3. ATBALSTS 4](#_Toc204683175)

[4. KONTROLES 4](#_Toc204683176)

[4.1. Informācijas sistēmas pārvaldība un politika 5](#_Toc204683177)

[4.2. Informācijas aktīvu pārvaldība 5](#_Toc204683178)

[4.3. Risku pārvaldība 5](#_Toc204683179)

[4.4. Fiziskā un vides drošība 5](#_Toc204683180)

[4.5. Piekļuves kontrole 5](#_Toc204683181)

[4.6. Cilvēkresursu drošība 5](#_Toc204683182)

[4.7. Apmācība un informētība 5](#_Toc204683183)

[4.8. Tīkla un darba staciju drošība 5](#_Toc204683184)

[4.9. Lietojumprogrammu drošība 6](#_Toc204683185)

[4.10. Konfigurācija pārvaldība 6](#_Toc204683186)

[4.11. Incidentu apstrāde 6](#_Toc204683187)

[4.12. Nepārtrauktība un krīzes vadība 6](#_Toc204683188)

[4.13. Kriptogrāfija 6](#_Toc204683189)

[4.14. Atbilstības un piegāžu ķēžu drošība 6](#_Toc204683190)

[4.15. Uzraudzība, žurnālfaili un auditi 6](#_Toc204683191)

[4.16. Datu rezerves kopēšana un atjaunošana 6](#_Toc204683192)

[4.17. Iznīcināšana 6](#_Toc204683193)

[4.18. Uzlabošana un korektīvās darbības 6](#_Toc204683194)

[5. IEKŠĒJĀS KONTROLES UN VĒRTĒŠANAS KĀRTĪBA 7](#_Toc204683195)

[5.1 Pašvērtējuma un atbilstības novērtējuma kārtība 7](#_Toc204683196)

[6. ĀRPAKALPOJUMA PĀRVALDĪBA 7](#_Toc204683197)

[Iekšējā audita kontroļu saraksts 9](#_Toc204683198)

# VISPĀRĒJĀS PRASĪBAS

Informācija par to, kā šī politika nosaka organizācijas vispārējo pieeju kiberdrošības procedūru īstenošanai, pamatojoties uz [Nacionālās kiberdrošības likumu](https://likumi.lv/ta/id/353390-nacionalas-kiberdrosibas-likums) un [25.06.2025. Ministru kabineta noteikumiem Nr. 397 “Minimālās kiberdrošības prasības”.](https://likumi.lv/ta/id/361481-minimalas-kiberdrosibas-prasibas)

Politika attiecas uz visiem darbiniekiem, nodarbinātajiem, struktūrvienībām, sistēmām un ārpakalpojumiem, kas izmanto vai pārvalda organizācijas informācijas un komunikāciju tehnoloģiju (IKT) resursus.

**Mērķis un piemērošanas joma**

Šīs politikas mērķis ir nodrošināt:

* Drošu, pārvaldītu un konsekventu kiberdrošības procedūru ieviešanu;
* Atbildību sadalījumu kiberdrošības pārvaldībā;
* Nepārtrauktu IKT resursu drošības uzraudzību, incidentu novēršanu un ziņošanu;
* Atbilstību normatīvajām prasībām un iekšējām kontroles procedūrām.

**Politikas piemērošanas joma attiecas uz:**

* Organizācijas IKT aktīviem (sistēmas, tīkli, dati);
* Būtisko un svarīgo pakalpojumu atbalsta procesiem;
* Globālās (izvietojums, kontrolējamā zona), lokālo (telpas un to piekļuves) un elektroniskās vides infrastruktūru (IAM, PAM utt.);
* Ārējiem piegādātājiem, kas apstrādā vai uztur informācijas sistēmas.

# INFORMĀCIJAS SISTĒMAS UN RISKU PĀRVALDĪBA

Informācija par to kā vadība uzņemas atbildību par kiberdrošības vadību, nodrošinot:

* kiberdrošības politikas **apstiprināšanu, ieviešanu un uzraudzību**;
* **resursu, līdzekļu un personāla** nodrošināšanu kiberdrošības pasākumu īstenošanai;
* **atbalstu kiberdrošības mērķu sasniegšanai** un to integrēšanu organizācijas stratēģijā;
* **informācijas drošības mērķu definēšanu** atbilstoši risku līmenim un pakalpojumu nozīmīgumam;
* pasākumus **aizsardzībai pret apdraudējumiem**, tostarp ievainojamību mazināšanai;
* **nepārtrauktības nodrošināšanu**, izstrādājot un uzturot kiberdrošības incidentu reaģēšanas un atjaunošanas plānus.

# PLĀNOŠANA

Informācija par to kā organizācijai jāizveido un jāuztur efektīva kiberdrošības plānošanas sistēma, kas ietver:

* **Riska pārvaldības procesu**, kas paredz risku identificēšanu, novērtēšanu, klasificēšanu un risinājumu izvēli;
* **Riska pieņemamības līmeņu noteikšanu** un risku pārvaldības stratēģiju īstenošanu;
* **Kiberdrošības mērķu noteikšanu**, piemēram:
  + apmācību programmu ieviešana,
  + uzbrukumu atklāšanas sistēmu ieviešana,
  + datu rezerves kopēšanas uzlabošana.

# ATBALSTS

Informācija par to lai nodrošinātu kiberdrošības pasākumu efektīvu ieviešanu, organizācija nodrošina:

* **kompetenču prasības –** darbiniekiem jābūt apmācītiem, informētiem un apzināties savas lomas un atbildību kiberdrošībā;
* **apmācību programmu uzturēšanu,** kas iekļauj sākotnējo un periodisko kiberdrošības apmācību;
* **dokumentācijas pārvaldību** – jāizstrādā, jāuztur un regulāri jāatjaunina šādi [dokumenti](https://likumi.lv/ta/id/361481#p21):
  + kiberdrošības politika;
  + IKT resursu un informācijas sistēmu katalogs;
  + kiberrisku izvērtējuma pārskati un pārvaldības plāns;
  + kiberincidentu reaģēšanas, darbības nepārtrauktības un atkopšanās plāni;
  + kiberincidentu žurnāli un procedūras.

# KONTROLES

Iekšējās tehnikas, taktikas un procedūras informācijas drošības un pakalpojumu pieejamības aizsardzībai.

## **Informācijas sistēmas pārvaldība un politika**

Organizācija nodrošina skaidri noteiktas lomas, atbildību un pilnvaras informācijas sistēmu pārvaldībā, balstoties uz apstiprinātu kiberdrošības politiku un pārvaldības struktūru.

## **Informācijas aktīvu pārvaldība**

Visi informācijas aktīvi tiek identificēti, klasificēti pēc kritiskuma, iekļauti resursu katalogā un aizsargāti atbilstoši to drošības klasei. Tiek pārvaldītas piekļuves, datu nesēji, nodošana un izmaiņas personālā.

## **Risku pārvaldība**

Riski tiek pārvaldīti visā sistēmas dzīves ciklā – sākot no konfigurācijas un ievainojamību izvērtēšanas līdz atjauninājumiem, ļaunatūras aizsardzībai, tīkla segmentācijai un drošības testiem. Riska izvērtējumi tiek regulāri pārskatīti un dokumentēti.

## **Fiziskā un vides drošība**

Organizācija nodrošina fizisko perimetru aizsardzību, zonējumu (administratīvās un paaugstinātas drošības zonas), drošu glabāšanu un aprīkojuma transportēšanu. Tiek ieviesti vides aizsardzības mehānismi, lai pārvaldītu fiziskus riskus infrastruktūrai.

## **Piekļuves kontrole**

Piekļuves tiesības tiek piešķirtas pēc nepieciešamības principa, ievērojot privilēģiju nodalīšanu. Tiek nodrošināta lietotāju autentifikācija, autorizācija un piekļuves žurnalēšana, lai nodrošinātu kontrolētu un izsekojamu darbību sistēmās.

## **Cilvēkresursu drošība**

Tiek īstenotas pārbaudītas procedūras personāla pieņemšanai, pārcelšanai un darba attiecību izbeigšanai, nodrošinot piekļuves kontroles aktualitāti un informācijas drošības saglabāšanu.

## **Apmācība un informētība**

Darbiniekiem tiek nodrošinātas regulāras kiberdrošības apmācības. Tiek īstenoti kiberhigiēnas pasākumi, lai veicinātu informētību un pārvaldītu cilvēkfaktora radītos apdraudējumus.

## **Tīkla un darba staciju drošība**

Tīkla infrastruktūra un galiekārtas tiek aizsargātas, attīstītas un uzturētas atbilstoši drošības prasībām, nodrošinot aizsardzību pret nesankcionētu piekļuvi un kiberuzbrukumiem.

## **Lietojumprogrammu drošība**

Lietojumprogrammu izstrāde un konfigurācija tiek veikta, ievērojot drošības prasības. Tiek veikta ievainojamību novēršana, testēšana un uzstādījumu pārvaldība, lai pārvaldītu riskus koda un sistēmu līmenī.

## **Konfigurācija pārvaldība**

Konsekventa sistēmu konfigurāciju pārvaldība nodrošina stabilu darbību, samazina kļūdu iespējamību un palīdz saglabāt drošības iestatījumu nemainību.

## **Incidentu apstrāde**

Tiek nodrošināta incidentu uzraudzība, ziņošana, novērtēšana un reaģēšana. Pēcincidentu analīze tiek izmantota uzlabošanai. Incidenti tiek klasificēti atbilstoši noteikumiem un dokumentēti žurnālā.

## **Nepārtrauktība un krīzes vadība**

Organizācijai ir izstrādāts nepārtrauktības un ārkārtas rīcības plāns, kā arī nodrošināta rezerves kopēšana un atkopšanās, lai saglabātu pakalpojumu pieejamību pēc incidentiem.

## **Kriptogrāfija**

Datu šifrēšana un atslēgu pārvaldība tiek veikta, lai aizsargātu konfidenciālu informāciju un nodrošinātu tās integritāti un nepieejamību neatļautām personām.

## **Atbilstības un piegāžu ķēžu drošība**

Organizācija ievēro normatīvās prasības un piemēro drošības standartus arī sadarbībā ar piegādātājiem, ierobežojot juridiskos un piegādes riskus.

## **Uzraudzība, žurnālfaili un auditi**

Regulāra sistēmu uzraudzība un žurnālu analīze palīdz atklāt anomālijas un kiberdraudus. Iekšējie un ārējie auditi pārbauda drošības kontroles efektivitāti.

## **Datu rezerves kopēšana un atjaunošana**

Rezerves kopijas tiek veiktas regulāri, pārbaudītas un glabātas droši, lai nodrošinātu datu pieejamību un ātru atjaunošanu pēc incidenta.

## **Iznīcināšana**

Datu un datu nesēju iznīcināšana notiek droši un dokumentēti, ievērojot datu aizsardzības un informācijas drošības prasības.

## **Uzlabošana un korektīvās darbības**

Tiek ieviestas korektīvās darbības pēc incidentiem, auditiem vai pārkāpumiem, nodrošinot nepārtrauktu kiberdrošības pārvaldības pilnveidi.

# IEKŠĒJĀS KONTROLES UN VĒRTĒŠANAS KĀRTĪBA

## 5.1 Pašvērtējuma un atbilstības novērtējuma kārtība

Organizācija nodrošina regulāru iekšējo kontroli un kiberdrošības efektivitātes izvērtēšanu, lai pārliecinātos par atbilstību noteiktajām prasībām un identificētu uzlabojumu iespējas.

Tiek veikti:

**Periodiski pasākumi:**

* kiberdrošības mērķu sasniegšanas izvērtējums, pamatojoties uz noteiktiem rādītājiem;
* iekšējie auditi, pārbaudot piekļuves tiesības, sistēmu konfigurācijas, incidentu apstrādi un dokumentācijas atbilstību;
* atbilstības novērtējumi pret 25.06.2025. Ministru kabineta noteikumu Nr. 397 “Minimālās kiberdrošības prasības” prasībām un citiem piemērojamajiem normatīvajiem aktiem, regulējumu vai standartiem.

**Nepārtraukti pasākumi:**

* neatbilstību novēršana, pamatojoties uz auditu, incidentu vai pārkāpumu rezultātiem;
* drošības mehānismu pilnveide, ņemot vērā jaunos apdraudējumus, ievainojamības un tehnoloģiju attīstību;
* pārskatīšana pēc būtiskiem kiberdrošības incidentiem, lai uzlabotu kontroles pasākumus un reaģēšanas gatavību.

# ĀRPAKALPOJUMA PĀRVALDĪBA

Līgumos ar ārpakalpojumu sniedzējiem par IKT resursa vai pakalpojuma iegādi obligāti jāiekļauj informācijas drošības un konfidencialitātes prasības, tajā skaitā:

* pieejas tiesību un datu apstrādes nosacījumi;
* apakšuzņēmēju piesaistes nosacījumi;
* incidentu ziņošanas pienākumi;
* audita tiesības un atbilstības kontrole.

Tiek īstenota **regulāra ārpakalpojuma sniedzēja darbības uzraudzība**, pārbaudot, vai tiek ievēroti līgumā noteiktie kiberdrošības nosacījumi un kvalitātes rādītāji, kā arī ārpakalpojuma izmantošana atbilst normatīvo aktu prasībām.

Ārpakalpojumiem jābūt iekļautiem organizācijas **nepārtrauktības un rezerves plānos**, lai kritisku pakalpojumu pārtraukuma gadījumā tiktu nodrošināta ātra atjaunošana.

Tiek dokumentēti un pārskatīti visi gadījumi, kad ārpakalpojumu sniedzējiem tiek uzticēta piekļuve:

* datiem, t.sk., personas datiem;
* informācijas sistēmām vai to daļām;
* iekšējiem procesiem, kas saistīti ar kiberdrošību.

Tiek nodrošināts, ka [pirms ārpakalpojuma līguma slēgšanas tas tiek saskaņots ar organizācijas kiberdrošības pārvaldnieku](https://likumi.lv/ta/id/361481#p92).

## Iekšējā audita kontroļu saraksts

|  |  |
| --- | --- |
| **Kategorija** | **Kontroles** |
| **Informācijas drošības pārvaldība un politika** (Organizācijai jāizstrādā, jāapstiprina un regulāri jāpārskata informācijas drošības politika.)  MK not. Nr. 397  3.3, 3.4., 3.5. apakšnodaļas | * Informācijas drošības politika un tās pārskatīšana |
| * Drošības mērķu izvirzīšana |
| * Aktīvu pārvaldība |
| * Riska un drošības kontroļu pārvaldība |
| * Nepārtrauktības pārvaldība |
| * Tehniskā atbilstības pārvaldība |
| * Juridiskā un normatīvā atbilstība |
| **Atbildības** (Pienākumi un saziņa.)  MK not. Nr. 397  3.5. un 3.6. apakšnodaļas | * Piekļuves kontrole (organizatoriska, fiziska, tehniska) |
| * Personāla drošība |
| * Komunikācija ar uzraugošajām iestādēm un informētība |
| **Informācijas aktīvu pārvaldība**  MK not. Nr. 397 | * Informācijas aktīvu katalogs |
| * Kiberriskam pakļauto aktīvu identificēšanā |
| * Informācijas un resursu lietošanas noteikumi |
| 3.4. apakšnodaļa | * Pieļaujamā informācijas un resursu lietošanas kārtība |
| * Aktīvu atgriešana |
| * Aktīvu klasificēšana |
| **Riska pārvaldība**  MK not. Nr. 397  3.5. apakšnodaļa | * Riska identificēšana, analīze un novēršana |
| **Fiziskā un vides drošība** (Fiziskās vides kontroles organizācijā, glabāšanā un transportā).  MK not. Nr. 397  3.7. apakšnodaļa | * Objektu un paaugstinātas drošības zonu aizsardzība |
| * Fiziskās vides kontroļu ieviešana un pārvaldība |
| **Piekļuves kontrole**  MK not. Nr. 397  3.7. apakšnodaļa | * Identitāšu pārvaldība |
| * Piekļuves tiesību un autentifikācijas mehānismi |
| * Priviliģētu lietotāju pārvaldība |
| * Priviliģētu utilītu programmu izmantošana |
| * Piekļuves kontrole nepriviliģētiem lietotājiem |
| **Cilvēkresursu Drošība** (Pārbaude uzsākot un pametot darbu)  MK not. Nr. 397  3.11. apakšnodaļa | * Pārbaudes uzsākot un pametot darbu |
| **Apmācība un informētība** (Izglītība, informētība un apmācība)  MK not. Nr. 397  3.11. apakšnodaļa | * Lietotāju apmācību plāni kiberdrošības jomā. * Kiberhigiēnas pasākumu īstenošanas kārtība |
| **Tīkla pārvaldība**  MK not. Nr. 397  3.8 apakšnodaļa | * Notikumu uzraudzība un tīkla drošība |
| * Tīkla pakalpojumu drošība |
| * Tīklu segregācija un segmentācija |
| * Tīmekļa filtrēšana |
| * Kriptogrāfijas lietošana (šifrēšana, kriptogrāfiska jaucējfunkcija) |
| * Drošs attīstītības dzīves cikls |
| **Uzraudzība un notikumu pārvaldība**  MK not. Nr. 397  3.9. apakšnodaļa | * Drošības uzraudzība |
| * Notikumu žurnālu vākšana un analīze |
| **Incidentu pārvaldība** (Jāizmeklē piekļuves kontroles pārkāpumi un jāveic korektīvie pasākumi.)  MK not. Nr. 397  3.6. apakšnodaļa, 7. nodaļa | * Incidentu pārvaldības procesi |
| * Reaģēšanas un ziņošanas procedūras |
| * Draudu medības un pierādījumu vākšana |
| * Mācīšanās no informācijas drošības incidentiem |
| * Pierādījumu vākšana |
| * Informācijas drošības notikumu ziņošana |
| **Nepārtrauktība un krīzes vadība**  (Jāveic regulāras datu rezerves kopijas un jānodrošina to atjaunošana. Jānodrošina kriptogrāfijas atslēgu droša pārvaldība un glabāšana.)  MK not. Nr. 397  3.5., 3.10., 3.12. apakšnodaļas | * IKT nepārtrauktības pārvaldība |
| * IKT gatavība pakalpojumu nepārtrauktībai |
| * Informācijas rezerves kopijas un integritātes saglabāšana |
| * Informācijas apstrādes iekārtu nepārtrauktība |
| * Integritātes saglabāšanas kontroles |
| * Konfidencialitātes un datu drošības saglabāšana datu pārraidē |
| * Konfidencialitātes un datu drošības saglabāšana glabāšanā |
| * Konfidencialitātes un datu drošības saglabāšana transportēšanā |
| * Darbības atjaunošana un ārkārtas plāni |
| **Lietojumprogrammu drošība**  MK not. Nr. 397  3.3., 3.7. apakšnodaļas, 4. nodaļa | * Lietojumprogrammu drošības prasības |
| * Droša sistēmas arhitektūra un inženierijas principi |
| * Droša programmēšana un testēšana |
| **Privātuma aizsardzība**  MK not. Nr. 397  3.3. apakšnodaļa | * Personas datu aizsardzība un maskēšana * Pseidonimizēšana, anonimizēšana |
| **Ievainojamību pārvaldība**  MK not. Nr. 397  3.3. un 3.5. apakšnodaļas | * Programmatūras ievainojamību analīze un pārvaldība |
| **Aizsardzība pret ļaunatūru**  MK not. Nr. 397  3.3. un 3.5. apakšnodaļas | * Ļaunatūras aizsardzības mehānismi |
| **Gala iekārtu pārvaldība**  MK not. Nr. 397  3.3, 3.4., 3.5., 3.8. apakšnodaļas | * Gala iekārtu konfigurācija un drošība |
| **Kriptogrāfija**  MK not. Nr. 397  3.12. apakšnodaļa | * Kriptogrāfijas lietošana, glabāšana un algoritmi |
| **Izmaiņu pārvaldība**  MK not. Nr. 397  3.3. apakšnodaļa | * Izmaiņu ieviešanas kontroles un pārvaldība |
| **Tiesību aktu un atbilstības prasības**  MK not. Nr. 397  3.3. apakšnodaļa | * Normatīvo prasību ievērošana un dokumentēšana |
| **Piegādātāju pārvaldība**  MK not. Nr. 397  4. nodaļa | * Drošības prasības piegādātajiem un mākoņpakalpojumiem |
| **Uzraudzība un auditi**  MK not. Nr. 397  8. nodaļa | * Regulāras pārbaudes un atbilstības novērtējumi. |
| * Riska analīze un iekšējās kontroles efektivitātes pārbaudes |
| * SIEM (Security Information and Event Management) drošības uzraudzība |
| * Dokumentēšana |
| **Datu rezerves kopēšana un atjaunošana**  MK not. Nr. 397  3.10. apakšnodaļa | * Regulāra datu rezerves kopēšana |
| * Šifrēšana un droša uzglabāšana |
| * Periodiska testēšana |
| **Iznīcināšana**  MK not. Nr. 397  3.5. apakšnodaļa | * Droša datu un fizisko nesēju iznīcināšana |
| **Uzlabošana un korektīvās darbības**  MK not. Nr. 397  3.5. un 3.6. apakšnodaļas | * Nepārtraukta uzlabošana un preventīvie pasākumi |