# Sistēmas drošības politika sistēmām RESURSI un PAKALPOJUMI

## 1. Sistēmas raksturojums un analīze drošības jomā

1.1. Drošības politika izstrādāta Iestādes informācijas un komunikācijas tehnoloģiju sistēmām RESURSI un PAKALPOJUMI.

1.2. Saskaņā ar Ministru kabineta 2015.gada 28.jūlija noteikumiem Nr.442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" sistēmas ir noteiktas kā pamata drošības sistēmas.

1.3. Sistēmu funkcijas:

1.3.1. RESURSI paredzēta Iestādes grāmatvedībai;

1.3.2. PAKALPOJUMI paredzēta normatīvos aktos noteikto Iestādes funkciju nodrošināšanai un pakalpojumu sniegšanai iedzīvotājiem.

1.4. Sistēmā apstrādā datus un informāciju, kas klasificēti kā "ierobežotas pieejamības" informācija.

1.5. Sistēmas lietotāji:

1.5.1. RESURSI lietotāji ir Iestādes vadība, grāmatvedība un iekšējais audits;

1.5.2. PAKALPOJUMI ir šādas lietotāju grupas:

1.5.2.1. Ārējie klienti - iedzīvotāji, kas noslēguši līgumu par Iestādes pakalpojumu saņemšanu;

1.5.2.2. Iestādes lietotāji - Iestādes Pakalpojumu nodaļas darbinieki.

1.6. Saistītās sistēmas:

1.6.1. RESURSI - nav saistīto sistēmu;

1.6.2. PAKALPOJUMI - saistītā sistēma ir www.iestāde.gov.lv.

1.7. Ārpakalpojumu sniedzēji:

1.7.1. RESURSI - nav ārpakalpojumu sniedzēju;

1.7.2. PAKALPOJUMI - sistēmas uzturēšanu nodrošina SIA "ĀRPAKALPOJUMU SNIEDZĒJS".

## 2. Sistēmas[1] drošības politikas mērķi un pamatnostādnes

2.1. Nodrošināt tādu informācijas tehnoloģiju vidi, lai Sistēma būtu aizsargāta pret ārējiem un iekšējiem drošības apdraudējumiem.

2.2. Apliecināt organizācijas vadības atbalstu Sistēmas drošības nodrošināšanai atbilstoši iestādes vajadzībām, saistošajiem normatīvajiem aktiem un drošības normām.

2.3. Sistēmas drošības politika ir saistoša visiem Sistēmu lietotājiem, kā arī SIA "ĀRPAKALPOJUMU SNIEDZĒJS".

## 3. Sistēmas drošības politikas uzdevumi:

3.1. Nodrošināt informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);

3.2. Nodrošināt informācijas integritāti (pilnīgas un nemainītas informācijas saglabāšanu);

3.3. Nodrošināt informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);

3.4. Aizsargāt Sistēmas informācijas resursus;

3.5. Aizsargāt Sistēmas tehniskos resursus;

3.6. Noteikt Sistēmas drošības apdraudējumus;

3.7. Novērtēt Sistēmas drošības riskus;

[1] Dokumentā, ja nav noteikts citādi, Sistēma attiecas uz abām sistēmām - RESURSI un PAKALPOJUMI

3.8. Atklāt Sistēmas drošības incidentus;
3.9. Atjaunot Sistēmas darbību pēc Sistēmas drošības incidentiem.

## 4. Sistēmas drošības pārvaldības organizācijas principi

4.1. Iestādē ir noteikts un regulāri tiek pilnveidots dokumentu un pasākumu kopums, kuru īstenošana nodrošina Sistēmas drošības politikas mērķa sasniegšanu.
4.2. Iestādē veicina katra darbinieka izpratni par pienākumiem risku un darbības nepārtrauktības pārvaldīšanā un informācijas un tehnoloģisko resursu aizsardzības nodrošināšanā, veicot Iestādes darbinieku regulāru izglītošanu.
4.3. Iestādē nodrošina pastāvīgu drošības politikas īstenošanas koordinēšanu un pārraudzīšanu.
4.4. Gadījumos, kad Iestādes darbinieki neievēro Drošības politikas izvirzītās prasības, Iestādes vadība var ierosināt disciplinārās atbildības procesu saskaņā ar esošajiem normatīvajiem aktiem.
4.5. Iestādē ir skaidri definēts un izprasts atbildības sadalījums par Sistēmas drošību.
4.6. Iestādes vadītājs:
- 4.6.1. Atbild par Sistēmas drošību;
- 4.6.2. Nosaka un apstiprina Sistēmas drošības politiku;
- 4.6.3. Nodrošina nepieciešamos līdzekļus un atbalstu Sistēmas drošības politikas ieviešanai, uzturēšanai un pilnveidošanai;
- 4.6.4. Nosaka pienākumu un atbildības sadalījumu attiecībā uz Sistēmas drošību:
  - 4.6.4.1. Atbildīgā persona par Sistēmu drošības pārvaldību ir Iestādes vadītāja vietnieks:
  - 4.6.4.2. Sistēmas tehnisko resursu valdītāji:
    - 4.6.4.2.1. RESURSI - Informātikas nodaļas vadītāja vietnieks;
    - 4.6.4.2.2. PAKALPOJUMI - Informācijas nodaļas vadītājs;
  - 4.6.4.3. Sistēmas informācijas resursu valdītāji:
    - 4.6.4.3.1. RESURSI - Grāmatvedības nodaļas vadītājs;
    - 4.6.4.3.2. PAKALPOJUMI - Pakalpojumu nodaļas vadītājs.

4.7. Atbildīgā persona par Sistēmas drošības pārvaldību:
- 4.7.1. Organizē Sistēmas risku analīzi;
- 4.7.2. Nodrošina nepieciešamo Sistēmas drošības dokumentu uzturēšanu un īstenošanu;
- 4.7.3. Veic noteikto drošības prasību ievērošanas uzraudzību un drošības incidentu izmeklēšanu;
- 4.7.4. Nodrošina darbinieku apmācību informācijas drošības jomā.

4.8. Sistēmas tehnisko resursu valdītājs:
- 4.8.1. Atbild par Sistēmas tehnisko resursu iegādi, izstrādi, darbību un uzturēšanu;
- 4.8.2. Nodrošina Sistēmas tehniskos un loģiskos aizsardzības pasākumus;
- 4.8.3. Atbild par Sistēmas pieejas tiesību pārvaldību;
- 4.8.4. Veic Sistēmas darbības atjaunošanas pasākumus, ja Sistēmas darbība ir traucēta.

4.9. Sistēmas informācijas resursu valdītājs:
- 4.9.1. Atbild par piekļuves kontroli informācijas resursam;
- 4.9.2. Klasificē viņa turējumā esošos informācijas resursus;
- 4.9.3. Nosaka drošības prasības informācijas resursam.

4.10. Lietotāji:
- 4.10.1. Iepazīstas un apņemas ievērot informācijas drošības jomā pieņemto iekšējo normatīvo aktu prasības;

4.10.2. Ziņo par Sistēmā identificētajiem riskiem, informācijas drošības notikumiem un incidentiem.

**5. Sistēmas drošības atbilstība normatīvajiem aktiem un standartiem**

5.1. Sistēma atbilst Latvijas Republikas tiesību aktiem informācijas drošības jomā.

**6. Sistēmas drošības principi**

6.1. Sistēmas lietotāju konti:

6.1.1. Sistēmas lietotāji, kas veic Sistēmas administrēšanas darbu, izmanto tam īpašus lietotāju kontus (turpmāk – Sistēmas administratora konti), kas netiek izmantoti ikdienas darbību veikšanai;

6.1.2. Katrs lietotāja konts ir saistīts ar konkrētu fizisko personu;

6.1.3. Sistēmkontus aizsargā tā, lai novērstu iespēju lietotājiem izmantot sistēmkontus.

6.2. Prasības parolēm:

6.2.1. Sistēmas piekļuve ir aizsargāta ar lietotāja vārdu un paroli;

6.2.2. Sistēmas lietotāju paroļu garums nav mazāks par deviņiem simboliem un satur vismaz lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un citu simbolu;

6.2.3. Sistēmas lietotāja paroles aizliegts glabāt un transportēt nešifrētā veidā, t.sk. lietotāja autentifikācijas procesa ietvaros;

6.2.4. Sistēmas lietotāja parole ievadīšanas brīdī netiek pilnībā attēlota lietotājam;

6.2.5. Sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir vienreiz lietojama;

6.2.6. Sistēmā nav funkcionalitātes, kas atļauj Sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;

6.2.7. Iekārtām, t.sk. infrastruktūras iekārtām, kas nodrošina sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles.

6.3. Izsekojamība:

6.3.1. Sistēmas auditācijas pierakstus veido un uzglabā vismaz 6 mēnešus pēc ieraksta izdarīšanas;

6.3.2. Jebkura piekļuve sistēmai ir izsekojama līdz konkrētam Sistēmas lietotāja kontam vai interneta protokola (IP) adresei.

6.4. Atjauninājumi:

6.4.1. Tehnisko resursu valdītājs sadarbībā ar atbildīgo par Sistēmas drošības pārvaldību veic pieejamo programmatūras atjauninājumu izvērtēšanu un nepieciešamības gadījumā - testēšanu;

6.4.2. Sistēmai nodrošina visus pieejamos nepieciešamos programmatūras atjauninājumus.

**7. Sistēmas aizsardzības pasākumi**

7.1. Visās Iestādes valdījumā esošajās gala lietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, uzstāda pretvīrusu aizsardzības sistēmu;

7.2. Sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamo tiesību kopu.

**8. Sistēmas drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamais līmenis**

8.1. Atbildīgais par Sistēmas drošības pārvaldību ne retāk kā reizi gadā veic Sistēmas drošības risku analīzi.

8.2. Risku analīzes ietvaros sadarbībā ar Iestādes vadītāju tiek veikts izvērtējums vai risku ierobežošanas un darbības nepārtrauktības nodrošināšanas izmaksas ir samērojamas ar

iespējamiem zaudējumiem, kas varētu rasties šo risku īstenošanās vai Iestādes darbības pārtraukšanas gadījumos.

**9. Sistēmas drošības kritēriji**

9.1. Sistēmas nepārtrauktās darbības laiks:

9.1.1. RESURSI - Sistēmai jābūt pieejamai darba dienās, darba laikā;

9.1.2. PAKALPOJUMI - Sistēmai jābūt pieejamai darba dienās, laikā no 8:00 līdz 20:00.

9.2. Sistēmas darbības atjaunošanas laiks:

9.2.1. RESURSI - Sistēmas darbība jāatjauno ne vēlāk kā 26 stundas pēc darbības pārtraukuma;

9.2.2. PAKALPOJUMI - Sistēmas darbība jāatjauno ne vēlāk kā 8 stundas pēc darbības pārtraukuma.

9.3. Nosacījumi, pie kuriem ikdienas procedūras aizstājamas ar krīzes pārvaldības procedūrām:

9.3.1. Ja Sistēmas darbības atjaunošanas laiks pārsniedz pieļaujamo;

9.3.2. Ja Sistēmā konstatēts datu zudums;

9.3.3. Ja RESURSI ilgāk par 8 stundām nav pieejama no ārējā tīkla.

**10. Noslēguma jautājumi**

10.1. Politiku pārskata vismaz reizi gadā, kā arī šādos gadījumos:

10.1.1. Ja izmaiņas Sistēmā var ietekmēt Sistēmas drošību;

10.1.2. Ja ir mainījušies vai atklāti jauni Sistēmas drošības apdraudējumi;

10.1.3. Ja pieaug Sistēmas drošības incidentu skaits vai noticis nozīmīgs Sistēmas drošības incidents;

10.2. Ja, pārskatot politiku, konstatēta atbilstoša nepieciešamība, to aktualizē.