Sistēmas drošības politika sistēmai PERSONĀLS

1. **Sistēmas raksturojums un analīze drošības jomā**
   1.1. Drošības politika izstrādāta Iestādes sistēmai PERSONĀLS (turpmāk - Sistēma).
   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" sistēma ir noteikta kā paaugstinātas drošības sistēma.
   1.3. Sistēma paredzēta Iestādes personāla uzskaitei.
   1.4. Sistēmā apstrādā datus un informāciju , kas klasificēta kā „ierobežotas pieejamības" informācija . Sistēmā apstrādā arī personas datus.
   1.5. Sistēmas lietotāji ir Iestādes Personāla nodaļas darbinieki.
   1.6. Saistītās sistēmas - sistēma RESURSI.
2. **Sistēmas 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 Sistēmas lietotājiem.
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;
   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 patstāvīgi 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 tehnisko 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 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 valdītājs ir IT nodaļas vadītājs;
4.6.4.3. Sistēmas informācijas resursu valdītājs ir Personāla nodaļas vadītājs.
4.7. Atbildīgā persona par Sistēmas drošības pārvaldību:
4.7.1. Organizē Sistēmas risku analīzes veikšanu;
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 pieejas kontroles politikas noteikšanu informācijas resursam;
4.9.2. Klasificē viņa pārziņā esošos informācijas resursus;
4.9.3. Nosaka drošības prasības informācijas resursam.
4.10. Lietotāji:
4.10.1. Iepazīstas un apņemas ievērot iekšējo normatīvo aktu prasības informācijas drošības jomā;
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:
5.1.1. Sistēmā ir ievērotas Latvijas Republikas normatīvo aktu prasības informācijas tehnoloģiju un informācijas drošības jomā (tostarp ievērotas fizisko personas datu aizsardzības prasības).
5.2. Sistēma atbilst starptautiskajiem normatīvajiem aktiem un standartiem 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 tos izmantot;
6.1.4. Ar administratora kontu piekļūt Sistēmai iespējams tikai izmantojot iekārtas, kas atrodas Iestādes kontrolētās telpās;
6.1.5. Sistēmas lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju - kļūdas apraksts un kļūdas identifikators.
6.2. Prasības parolēm:

6.2.1. Piekļuve Sistēmai ir aizsargāta ar lietotāja vārdu un paroli;
6.2.2. Sistēmas lietotāja 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. Katram Sistēmas lietotājam parole ir obligāti jāmaina pēc ne vairāk kā 90 dienām;
6.2.4. Piecas secīgas reizes nepareizi ievadot sistēmas lietotāja konta paroli, šis konts (izņemot Sistēmas administratora kontu) nekavējoties tiek bloķēts;
6.2.5. Sistēmas lietotāja paroles aizliegts glabāt un transportēt nešifrētā veidā, t.sk. lietotāja autentifikācijas procesa ietvaros;
6.2.6. Sistēmas lietotāja parole tās ievadīšanas brīdī netiek pilnībā attēlota lietotājam;
6.2.7. Sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir vienreiz lietojama;
6.2.8. Sistēmā nav funkcionalitātes, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;
6.2.9. Tehnisko resursu valdītājs nodrošina, ka iekārtām, t.sk. infrastruktūras iekārtām, kas nodrošina Sistēmas funkcionēšanu (SERVERIS 1), netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles.

6.3. Izsekojamība:
6.3.1. Tiek nodrošināta sistēmas pierakstu veidošana un uzglabāšana vismaz 18 mēnešus pēc ieraksta izdarīšanas, uzglabājot pierakstu kopijas atsevišķi no Sistēmas Personāla nodaļas vadītāja seifā;
6.3.2. Sistēmas pieraksti tiek veidoti, nodrošinot, ka ierakstā norādītais laiks sakrīt ar faktiskā notikuma koordinēto universālo laiku (UTC) ar vienas sekundes precizitāti izmantojot NTP serveri 0.lvUNIVERSALAIS LAIKS.pool.ntp.org;
6.3.3. Atbildīgā persona par Sistēmas drošības pārvaldību nodrošina Sistēmas auditācijas pierakstu satura plānveida uzraudzību un analīzi, lai konstatētu incidentus;
6.3.4. 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 jābūt uzliktiem visiem pieejamajiem nepieciešamajiem programmatūras atjauninājumiem.

7. **Sistēmas aizsardzības pasākumi**

7.1. Visās Iestādes valdījumā esošajās gala lietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, ir iekļauta pretvīrusu funkcionalitāte, izmantojot ANTIVĪRUSS 2016 risinājumu;
7.2. Sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamo tiesību kopu;
7.3. Fiziski piekļūt iekārtām, kas nodrošina Sistēmas darbību, atļauts vienīgi iestādes pilnvarotām personām vai šo personu pavadībā;
7.4. Plūsma starp informācijas sistēmu un tās lietotājiem, kā arī starp informācijas sistēmu un citām informācijas sistēmām tiek kontrolēta, izmantojot ugunsmūra risinājumu UGUNSMŪRIS 2016;
7.5. Ir atslēgti šādi datortīkla pakalpojumi (network services), kas netiek izmantoti sistēmas darbības nodrošināšanai:

7.5.1. /etc/services/PAKALPOJUMS 99;
7.5.2. /etc/services/PAKALPOJUMS 22.

7.6. Veicot Sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu sistēmās glabāto datu integritātei, tādēļ šādiem nolūkiem ir izveidota sistēmas TESTA VIDE;

7.7. Sistēmas izvietošana ārpakalpojumu sniedzēja nodrošinātos resursos atļauta tikai tad, ja pakalpojumu sniedzējs ir juridiska persona, kas reģistrēta Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, un Sistēmā glabātā informācija atrodas vienīgi Eiropas Savienības vai Eiropas Ekonomikas zonas valstu teritorijā.

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

9.1.1. Sistēma ir pieejama darba dienās darba laikā.

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

9.1.2.1. Ja Sistēmas darbības atjaunošanas laiks pārsniedz pieļaujamo;

9.1.2.2. Ja Sistēmā konstatēts datu zudums.

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 aktualizēt.