Drošības riska pārvaldības plāns Iestādes informācijas sistēmai

1. **Vispārīgie jautājumi**
   1.1. Drošības riska pārvaldības plāns izstrādāts Iestādes informācijas sistēmai (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.
2. **Risku analīzes metodoloģija**
   2.1. Risku analīzes mērķi Iestādē ir:
      2.1.1. Apzināt Sistēmas risku līmeni;
      2.1.2. Noteikt kādas darbības veicamas Sistēmas risku pārvaldībai:
         2.1.2.1. Riska pieņemšana;
         2.1.2.2. Izvairīšanās no riska;
         2.1.2.3. Riska mazināšanas pasākumi;
         2.1.2.4. Riska nodošana trešajai pusei.
   2.2. Risku analīze ir jāveic visā Sistēmas dzīves ciklā ar šajā plānā noteikto regularitāti.
   2.3. Risku analīzes veikšanā izmanto Sistēmas drošības apdraudējumu uzskaitījumu.
   2.4. Risku analīzes veikšanu nodrošina Atbildīgā persona par Sistēmas drošības pārvaldību, iesaistot vismaz:
      2.4.1. Sistēmas informācijas resursu valdītāju;
      2.4.2. Sistēmas tehnisko resursu valdītāju.
   2.5. Riska mazināšanas pasākumi tiek noteikti, pamatojoties uz to izmaksu un iespējamo zaudējumu samērojamību.
   2.6. Katram riska mazināšanas pasākumam Iestādē tiek noteikts vismaz ieviešanas termiņš un atbildīgais par ieviešanu.
   2.7. Atbildīgā persona par Sistēmas drošības pārvaldību kontrolē risku mazināšanas pasākumu ieviešanu.
3. **Sistēmas drošības risku analīzes apraksts**
   3.1. Apdraudējuma varbūtību (AV) nosaka, izmantojot skalu:
      3.1.1. Maza apdraudējuma varbūtība (1) – iespējams, ka apdraudējums īstenosies reizi 10 gados/ 10 % iespējamo gadījumu;
      3.1.2. Neliela apdraudējuma varbūtība (2) - iespējams, ka apdraudējums īstenosies reizi 5 gados/ 25 % iespējamo gadījumu;
      3.1.3. Vidēja apdraudējuma varbūtība (3) - iespējams, ka apdraudējums īstenosies reizi gadā/ 50 % iespējamo gadījumu;
      3.1.4. Ievērojama apdraudējuma varbūtība (4) – iespējams, ka apdraudējums īstenosies reizi mēnesī / 75 % iespējamo gadījumu;
      3.1.5. Liela apdraudējuma varbūtība (5) – iespējams, ka apdraudējums iestāsies lielākajā daļā gadījumu vai katru dienu.
   3.2. Kaitējumu (RK) no katra apdraudējuma nosaka, izmantojot skalu:
      3.2.1. Mazs kaitējums (1)– atsevišķas problēmas iekšējiem lietotājiem;
      3.2.2. Neliels kaitējums (2) –atsevišķas problēmas iekšējiem un ārējiem klientiem vai sadarbības partneriem;
      3.2.3. Vidējs kaitējums (3) – apgrūtināta Iestādes darbība, atsevišķi datu integritātes vai pieejamības traucējumi;

3.2.4. Ievērojams kaitējums (4)– Iestādes darbības pārtraukums līdz 24 stundām/ pilnīgs resursa zudums/ ierobežotas pieejamības informācijas noplūde;

3.2.5. Liels kaitējums (5) – pilnīgs Iestādes darbības pārtraukums uz ilgāku laiku kā 24 stundas/ informācijas dienesta vajadzībām noplūde.

3.3. Riska aprēķināšanu veic - risks= (apdraudējuma varbūtība x resursa apdraudējuma kaitējums). R=AVxRK .

3.4. Riska novērtējuma skala:

3.4.1. No 1 līdz 9 –neliels risks tiek akceptēts un pieņemts, drošības pasākumu veikšana nav nepieciešama;

3.4.2. No 10 līdz 16 – augsts risks, drošības pasākumus nepieciešams veikt ne vēlāk kā līdz nākamajai risku analīzei (1 gada laikā);

3.4.3. No 17 līdz 25 – ļoti augsts risks, drošības pasākumi jāveic nekavējoties, bet ne vēlāk kā 3 mēnešu laikā.

3.5. Atbildīgā persona par Sistēmas drošības pārvaldību apkopo drošības pasākumus, norādot izmaksas, termiņu un atbildīgo par pasākuma ieviešanu.

4. Sistēmas drošības apdraudējumi

4.1. Iestāde sagatavo Sistēmas drošības apdraudējumu uzskaitījumu.

4.2. Apskata vismaz šādu kategoriju drošības apdraudējumus:

4.2.1. Ar aparatūru saistītie apdraudējumi;

4.2.2. Ar programmatūru saistītie apdraudējumi;

4.2.3. Ar Iestādes personālu saistītie apdraudējumi;

4.2.4. Ar komunikācijām saistītie apdraudējumi;

4.2.5. Apkārtējās vides apdraudējumi.

4.3. Veicot risku analīzi, apskata katra apdraudējuma īstenošanās varbūtības novērtējumu un tuvošanās pazīmju uzskaitījumu.

4.4. Apdraudējumu piemēri uzskaitīti 1.pielikumā.

5. Sistēmas drošības riska novērtējums

5.1. Sistēmas drošības risku novērtējumam aizpilda šādu tabulu:

Nr.	Apdraudējums	Apraksts	Apdraudējuma varbūtība	Kaitējums	Riska novērtējums

5.2. Kaitējuma sadaļā apskata Iestādes, sistēmas datu subjektu un sistēmas lietotāju iespējamo zaudējumu vai kaitējuma novērtējumu, ja notiktu Sistēmas drošības incidents attiecīgā apdraudējuma rezultātā.

6. Sistēmas drošības riska mazināšanas pasākumi

6.1. Sistēmas drošības riska mazināšanai aizpilda šādu tabulu:

Nr	Apdraudējums	Drošības pasākuma apraksts	Ieviešanas termiņš	Izmaksas vai citi nepieciešamie līdzekļi	Izpildītājs

7. Sistēmas drošības riska mazināšanai veikto pasākumu lietderības novērtējums

7.1. Katras nākamās risku analīzes laikā Atbildīgā persona par Sistēmas drošības pārvaldību novērtē katru riska mazināšanai veikto pasākumu lietderību.

7.2. Gadījumā, ja riska mazināšanas pasākums ir bijis nelietderīgs (piemēram, attiecīgais riska līmenis nav samazinājies), nosaka citu risku mazināšanas pasākumu.

8. Noslēguma jautājumi

8.1. Plānu pārskata vismaz reizi gadā, kā arī šādos gadījumos:

8.1.1. Ja izmaiņas Sistēmā var ietekmēt Sistēmas drošību;

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

8.1.3. Ja pieaug Sistēmas drošības incidentu skaits vai noticis nozīmīgs Sistēmas drošības incidents.

8.2. Ja, pārskatot plānu, konstatēta atbilstoša nepieciešamība, to aktualizē.

1.Pielikums

1. **Ar aparatūru saistītie apdraudējumi,**

Apkalpošanas kļūda
Aparatūras nepietiekama veiktspēja
Aparatūras atteice
Neautorizētas darbības ar datu nesējiem
Datu nesēju nepareiza glabāšana
Rezerves kopiju atjaunošanas problēmas
Piegāžu ķēdes un ar izstrādātājiem saistītie riski
..

2. **Ar programmatūru saistītie apdraudējumi,**

Programmatūras kļūda
Ieviešanas kļūda
Uzturēšanas kļūda
Nelicencētas programmatūras lietošana
Neaktuāla programmatūras dokumentācija
Piegāžu ķēdes un ar izstrādātājiem saistītie riski
..

3. **Ar Iestādes personālu saistītie apdraudējumi**

Neautorizētas darbības
Paroles izpaušana
Svešas identitātes izmantošana
Paroļu politika
Personāla trūkums
Lietotāju kļūdas
Informācijas izpaušana
..

4. **Ar komunikācijām saistītie apdraudējumi**

Komunikāciju līniju bojājumi
Pārraides kļūda
Kļūda ziņojumu adresācijā
Datu plūsmas pārslodze
Atkarība no citām sistēmām
..

5. **Apkārtējās vides apdraudējumi**

Ugunsgrēks
Plūdi
Zibens
Vētra
Zādzība
Sprādziens
Tīšs bojājums
Putekļi
Temperatūras ekstrēmi
Mitruma ekstrēmi

Sprieguma svārstības

..