Sistēmas drošības iekšējie noteikumi sistēmai PERSONĀLS

1. **Vispārīgie jautājumi**
   1.1. Drošības riska pārvaldības plāns izstrādāts 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. Sistēmas informācijas resursi:
      1.3.1. Personāla uzskaites dati;
      1.3.2. Darba aizsardzības dati.
   1.4. Sistēmas tehniskie resursi:
      1.4.1. SERVERIS 88;
      1.4.2. SERVERIS TESTS.
2. **Informācijas sistēmas dzīves cikls**
   2.1. Veicot Sistēmas izstrādes, iegādes, ieviešanas un pārmaiņu pārvaldīšanas procesu, Iestāde ievēro un atbild par Informācijas sistēmas drošības prasību ievērošanu neatkarīgi no tā, vai šos procesus veic Iestāde vai ārējais izstrādātājs un piegādātājs.
   2.2. Iestāde dokumentē Sistēmas izstrādes, iegādes, ieviešanas un pārmaiņu pārvaldīšanas norisi.
   2.3. Iestāde nosaka par Sistēmu atbildīgās personas:
      2.3.1. Informācijas resursu valdītājs - pakalpojumu nodaļas vadītāja vietnieks;
      2.3.2. Tehnisko resursu valdītājs - IT nodaļas vadītājs;
      2.3.3. Atbildīgā persona par Sistēmas drošības pārvadību - Iestādes vadītāja vietnieks.
   2.4. Atbildīgās personas nosaka Sistēmas drošības prasības un risku ierobežošanas pasākumus.
   2.5. Sistēmas izstrādes videi ir jāatbilst drošības prasībām, un tai jābūt nodalītai no produkcijas vides.
   2.6. Pieejas tiesības Sistēmas izstrādes videi nosaka atbilstoši personu pienākumiem.
   2.7. IT nodaļa nodrošina Sistēmas dokumentācijas sagatavošanu un uzturēšanu.
   2.8. Dokumentācijā iekļauj nepieciešamo informācijas apjomu, lai varētu kvalitatīvi veikt Sistēmas lietošanu, uzturēšanu un pārmaiņu pārvaldīšanu.
   2.9. Pirms Sistēmas ieviešanas IT nodaļa veic Sistēmas darbības funkcionalitātes un drošības atbilstības noteiktajām prasībām pārbaudi.
   2.10. Pārbaudē piedalās personas, kas ir noteikušas funkcionalitātes un drošības prasības, informācijas resursu turētāji un lietotāji.
   2.11. Pamatojoties uz Pārbaudes rezultātiem, IT nodaļa nodrošina Sistēmas koriģēšanu vai uzsāk tās ieviešanu.
   2.12. Sistēmas ieviešana:
      2.12.1. Sistēmu ievieš, saņemot saskaņojumu no tiem informācijas resursu turētājiem, kuru Informācijas resursi tiks ietekmēti;
      2.12.2. Pirms Sistēmas nodošanas lietošanā atbildīgās personas veic darbinieku apmācību un citus pasākumus, lai nodrošinātu darbinieku izpratni par Informācijas sistēmas lietošanu, aizsardzības pasākumiem un to nozīmīgumu;

2.12.3. Ieviešot Sistēmu, tajā nedrīkst būt testētāju lietotāja konti un testēšanas datu faili;
2.12.4. IT nodaļa nodrošina, lai tiktu saglabāti ieviestās Sistēmas pirmkodi.

2.13. Sistēmas izmaiņu pārvaldība :

2.13.1. Sistēmas pārmaiņas tiek veiktas ar visu saistīto informācijas resursu turētāju atļauju;
2.13.2. IT nodaļa identificē visus informācijas un tehniskos resursus, kurus ietekmē pārmaiņas;
2.13.3. Atbildīgais par Sistēmas drošības pārvaldību analizē, kā pārmaiņas ietekmēs esošos informācijas sistēmas drošības pasākumus un vai pārmaiņu rezultātā nesamazināsies informācijas sistēmas drošības līmenis;
2.13.4. IT nodaļa veic informācijas sistēmas dokumentācijas papildināšanu;
2.13.5. IT nodaļa uztur visu pārmaiņu reģistrācijas žurnālu;
2.13.6. Pirms izmaiņu ieviešanas veido rezerves kopijas tiem informācijas resursiem, kurus var ietekmēt izmaiņas;
2.13.7. Pēc izmaiņu ieviešanas Informācijas resursu valdītājs pārliecinās, vai informācijas sistēmas pārmaiņu rezultātā ir saglabāta datu integritāte;
2.13.8. Atbildīgais par Sistēmas drošības pārvaldību izstrādā procedūru par darbībām ārkārtas (neplānotu) pārmaiņu apstākļos un nosaka, kas ir tiesīgs pieņemt lēmumu par ārkārtas pārmaiņām.

2.14. Sistēmas lietošanas izbeigšana:

2.14.1. Likvidējot Sistēmu vai, nododot to citai personai, iestāde veic nepieciešamos drošības pasākumus;
2.14.2. Pirms Sistēmas likvidācijas, Iestāde veic risku analīzi, kurā izvērtē iespējamo apdraudējumu citām Informācijas sistēmām un |Iestādei kopumā;
2.14.3. Iestādei jānosaka turpmākās darbības ar Sistēmu - pilnīga likvidēšana vai glabāšana arhīvā;
2.14.4. Ja Sistēmu pilnībā likvidē, Iestāde nodrošina tajā ietilpstošo informācijas resursu likvidēšanu;
2.14.5. Ja Sistēmu ievieto arhīvā, Iestāde nodrošina noteikto Sistēmas drošības līmeni un likvidē lietošanas tiesības, kuras var atjaunot vēsturisko datu caurskatīšanai ar Informācijas resursu turētāja vai iestādes vadītāja lēmumu.

3. Piekļuves kontrole

3.1. Piekļuves tiesības apstiprina Informācijas resursu valdītājs. Balstoties uz Informācijas resursu valdītāja apstiprinātu pieprasījumu, Tehnisko resursu valdītājs izveido lietotājam piekļuvi.
3.2. Informācijas resursu valdītājs ir atbildīgs par Tehnisko resursu valdītāja informēšanu par lietotājiem, kuri pārtrauc vai maina darba attiecības ar Iestādi. Tehnisko resursu valdītājs pēc šīs informācijas saņemšanas nekavējoties anulē vai izmaina attiecīgā darbinieka piekļuves tiesības.
3.3. Lietotājs ir atbildīgs par darbībām, kas tiek veiktas, izmantojot viņa lietotājvārdu (identifikatoru).
3.4. Lietotājs paroli maina vismaz reizi 3 mēnešos.

3.5. Tehnisko resursu valdītājs nodrošina:
3.5.1. Automātisku paroles maiņas pieprasījumu, lietotājam pirmo reizi reģistrējoties tīklā;
3.5.2. Automātisku paroles maiņas pieprasījumu ik pēc 3 mēnešiem;
3.5.3. Sistēmas bloķēšanu, ja lietotājs piecas reizes pēc kārtas ir ievadījis nepareizu paroli vai lietotājvārdu.
3.6. Rakstiskā veidā paroles atļauts glabāt tikai aizslēgtā seifā vai izmantojot drošības pārvaldnieka apstiprinātus elektroniskus saglabāšanas līdzekļus.
3.7. Ja radušās aizdomas, ka paroli uzzinājusi cita persona, lietotājs to nekavējoties nomaina un par incidentu ziņo drošības pārvaldniekam.
3.8. Aizliegts mēģināt uzzināt citu lietotāju paroles, izņemot gadījumus, kad tas ir nepieciešams Tehnisko resursu valdītājam viņa tiešo pienākumu veikšanai. Pēc minēto darbu pabeigšanas lietotāja parole tiek nomainīta.
3.9. Uz datora ir jābūt uzstādītam ekrāna saudzētājam ar aktivizācijas paroli. Tam ir automātiski jāaktivizējas, ja piecu minūšu laikā lietotājs nav veicis nekādas darbības.
3.10. Tehnisko resursu valdītājam ir tiesības veikt lietotāju darbības auditus. Šādi auditi var ietvert lietotāja darbību auditācijas veikšanu.

4. Informācijas resursu rezerves kopijas

4.1. Lietotāja līmeņa informācijai (piemēram, lietotāja ievadītie dati) Iestāde veido regulāras rezerves kopijas.
4.2. Sistēmas līmeņa informācijai, tehnisko resursu konfigurācijai un Sistēmas dokumentācijai iestāde veido regulāras rezerves kopijas.
4.3. Rezerves kopijas tiek uzglabātas:
4.3.1. Iestādē;
4.3.2. Ģeogrāfiski attālinātā vietā.
4.4. Atbildīgais par Sistēmas drošības pārvaldību, nepieciešamības gadījumā piesaistot Informācijas resursu un Tehnisko resursu valdītāju, izstrādā rezerves kopiju izgatavošanas un Sistēmas atjaunošanas kārtību, kurā nosaka rezerves kopiju veikšanas biežumu, apjomu, uzglabāšanas kārtību.
4.5. IT nodaļa ne retāk kā reizi ceturksnī veic rezerves kopiju lasīšanas pārbaudi.
4.6. IT nodaļa ne retāk kā reizi gadā veic pilnu Sistēmas informācijas atjaunošanas testu.
4.7. IT nodaļa nodrošina rezerves kopiju aizsardzību pret neautorizētu piekļuvi.

5. Datu nesēji

5.1. Iestāde marķē visus ārējos datu nesējus, kuros ir klasificēta informācija atbilstoši Iestādes noteiktajai informācijas klasifikācijai.
5.2. Marķējumā norāda vismaz:
5.2.1. Informācijas klasifikācijas līmeni;
5.2.2. Informācijas identifikatoru.
5.3. Izņēmums - datu nesējus pieļaujams nemarķēt, ja tie atrodas serveru telpā.
5.4. Datu nesēji tiek uzglabāti 105.telpā.
5.5. Transportējot datu nesējus ārpus Iestādes kontrolētās zonas, Iestāde nodrošina skaidri noteiktu atbildību par attiecīgā datu nesēja transportēšanu, kā arī atbilstošu pierakstu veikšanu.

5.6. IT nodaļa nodrošina datu nesēju aizsardzību pret neautorizētu piekļuvi.

6. Piekļuves dati un Sistēmas informācija

6.1. IT nodaļa uztur Sistēmas dokumentāciju, kas apraksta vismaz:

6.1.1. Sistēmas vai Sistēmas komponenšu drošu konfigurāciju, instalēšanu un darbību;

6.1.2. Sistēmas drošības mehānismu izmantošanu un uzturēšanu;

6.1.3. Administratīvo / priviliģēto funkciju izmantošanu.

6.2. Sistēmas dokumentācijai Iestāde nosaka atbilstošu klasifikācijas līmeni un nodrošina šīs informācijas vai datu atbilstošu aizsardzību un glabāšanu.

7. Loģiskā aizsardzība

7.1. Iestāde dokumentē un veic informācijas sistēmu loģiskās aizsardzības pasākumus.

7.2. Iestāde dokumentē Sistēmas lietotāju reģistrācijas, tiesību piešķiršanas un anulēšanas procesu.

7.3. Lietotājam tiek piešķirts unikāls lietotāja kods un parole.

7.4. Lietotāja reģistrāciju veic saskaņā ar drošības politiku.

7.5. Lietotāja darba pienākumu maiņas vai darba attiecību izbeigšanas gadījumā tiek nekavējoties mainīti vai anulēti piešķirtie lietotāja kodi un pieejas tiesības Sistēmai.

7.6. Priviliģēto lietotāju pieejas kodus kopā ar parolēm glabā seifā 106. telpā.

7.7. Autentifikācijas līdzekļu lietošanas veidus un kārtību nosaka Atbildīgais par Sistēmas drošību, un tehniski to nodrošina Tehnisko resursu valdītājs.

7.8. Iestāde pēc nepieciešamības veic papildu loģiskās aizsardzības pasākumus atkarībā no Informācijas sistēmas resursu klasifikācijas līmeņa.

7.9. Iestāde veic līdzvērtīgus loģiskās aizsardzības pasākumus vienā līmenī klasificētiem Informācijas resursiem neatkarīgi no datu glabāšanas veida.

7.10. Ārpakalpojumu sniedzējam jānodrošina Sistēmas drošības līmenis, kas nav zemāks par šajos noteikumos noteikto.

8. Fiziskā aizsardzība

8.1. Iestāde aizsargā Sistēmu no fiziskiem un ārējās vides apdraudējumiem.

8.2. Iestāde izstrādā un uztur aktuālu sarakstu ar personām, kam tiesības fiziski piekļūt telpām, kur atrodas tehniskie resursi, kā arī nodrošina tiem attiecīgus piekļuves līdzekļus.

8.3. Iestāde nodrošina piekļuves līdzekļu maiņu gadījumā, ja ir aizdomas par to nozaudēšanu vai neautorizētu izmantošanu.

8.4. Iestāde uztur žurnālierakstus par fizisko piekļuvi telpām, kur atrodas tehniskie resursi.

8.5. Apmeklētāju piekļuvi Sistēmai saskaņo ar Informācijas resursu valdītāju, un apmeklētāju pavada persona, kas autorizēta piekļūt Sistēmai.

8.6. Tehnisko resursu valdītājs ir atbildīgs par tehnisko resursu pietiekamu fizisko aizsardzību pret fiziskiem apdraudējumiem, izvērtējot iespējamos zaudējumus, izmantojot šādus līdzekļus:

8.6.1. Ugunsdzēsības signalizāciju;

8.6.2. Pretielaušanās signalizāciju;

8.6.3. Alternatīvo elektrības barošanu;

8.6.4. Automātiskās ugunsdzēsības sistēmas;

8.6.5. Dzesēšanas iekārtas;

8.6.6. Automatizētas telpas apstākļu (temperatūras, mitruma) mērīšanas iekārtas.

9. Apdraudējumu un incidentu pārvaldība

9.1. Atbildīgais par Sistēmas drošības pārvaldību sadarbībā ar Tehnisko resursu valdītāju seko līdzi informācijai par jaunākajām drošības ievainojamībām, Sistēmas ražotāja drošības paziņojumiem, CERT.LV paziņojumiem, kas varētu liecināt par Sistēmas drošības apdraudējumiem.

9.2. Informācijas sistēmas drošības apdraudējuma pazīmes nosaka, veicot nepārtrauktu informācijas sistēmas resursu uzraudzību, kas nodrošina automātisku paziņošanu, potenciālā apdraudējuma iespējamībai sasniedzot noteiktus parametrus.

9.3. Sistēmu aizsardzībai tiek izmantota Ielaušanās noteikšanas sistēma (IDS).

9.4. Iestādes darbinieks, pamanot iespējamu apdraudējumu vai incidentu, nekavējoties par to ziņo Atbildīgajam par Sistēmas drošību vai Iestādes vadībai.

9.5. Atbildīgais par Sistēmas drošību nodrošina drošības incidentu uzskaiti un analīzi.

9.6. Atbildīgais par Sistēmas drošību nodrošina pasākumu izstrādāšanu, lai novērstu drošības incidenta radītās sekas un nepieļautu līdzīgu incidentu atkārtošanos.

9.7. Atbildīgais par Sistēmas drošību nodrošina drošības incidentu paziņošanu CERT.LV atbilstoši normatīvo aktu prasībām.

9.8. Par fiziskās aizsardzības pārkāpumiem un to radītajām sekām darbiniekam nekavējoties jārīkojas atbilstoši iekšējo normatīvo aktu noteiktajai kārtībai un jāpaziņo savas struktūrvienības vadītājam.

10. Sistēmas darbība, ja resursi pieejami nepilnā apjomā

10.1. Sistēmas minimālās funkcijas - personālvadības modulis.

10.2. Sistēmas pārējās funkcijas - darba aizsardzības modulis.

10.3. Gadījumā, ja nav pieejamas sistēmas funkcijas, tiek īstenoti darbības atjaunošanas pasākumi saskaņā ar noteikto kārtību.

11. Tehnisko resursu izmaiņu pārvaldība

11.1. Iestādē formāli tiek pārvaldītas šādas izmaiņas tehniskajos resursos:

11.1.1. izmaiņas tehnisko resursu komplektācijā;

11.1.2. izmaiņas tehnisko resursu darbībā;

11.1.3. jaunu tehnisko resursu iekļaušana Sistēmā.

11.2. Tehnisko izmaiņu veikšanu atbilstoši savai kompetencei veic šādi Iestādes darbinieki:

11.2.1. Tehnisko resursu valdītājs;

11.2.2. Sistēmas administrators, saskaņojot ar Tehnisko resursu valdītāju;

11.2.3. Ārpakalpojumu sniedzējs atbilstoši noslēgtajos līgumos noteiktajai kārtībai.

11.3. Tehnisko resursu izmaiņas nepieciešams saskaņot ar ietekmēto Informācijas resursu valdītāju.

11.4. Iestāde nodrošina izmaiņu uzskaiti un izsekojamību.

12. Darbinieku apmācības

12.1. Atbildīgais par Sistēmas drošību nodrošina pamata informācijas drošības apmācību lietotājiem ne retāk kā reizi gadā, kā arī šādos gadījumos:

12.1.1. Kā daļu no apmācībām, uzsākot darbu Iestādē;

12.1.2. Būtisku Sistēmas izmaiņu gadījumos.

12.2. Iestāde saglabā pierakstus par darbinieku dalību informācijas drošības mācībās.

13. Atjauninājumu pārvaldība

13.1. Pirms atjauninājumu uzstādīšanas sistēmai :

13.1.1. Pārliecinās, ka atjauninājumi nemazina sistēmas drošības līmeni vai zudumu iespējams kompensēt ar adekvātām kontrolēm, kas mazina risku;

13.1.2. Sisitēmas pārmaiņas veic organizēti un atbilstoši iestādes IS drošības politikas uzstādījumiem;

13.1.3. Sistēmas pārzinis un tehnisko resursu turētājs/-i ir informēti par uzstādāmajām pārmaiņām.

14. Auditācija

14.1. Iestāde nodrošina Sistēmas auditācijas pierakstus par:

14.1.1. Nesekmīgiem pieslēgšanās mēģinājumiem;

14.1.2. Paroļu maiņa.

14.2. Auditācijas pieraksti satur informāciju par notikumu, laiku, ar notikumu saistīto lietotāju.

14.3. Iestāde nodrošina Sistēmas auditācijas pierakstu uzglabāšanu 18 mēnešus pēc notikuma.

14.4. Atbildīgais par Sistēmas drošību nodrošina regulāru Sistēmas auditācijas pierakstu uzraudzību un analīzi, lai konstatētu incidentus.

15. Noslēguma jautājumi

15.1. Noteikumus pārskata vismaz reizi gadā, kā arī šādos gadījumos:

15.1.1. Ja izmaiņas Sistēmā var ietekmēt Sistēmas drošību;

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

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

15.1.4. Ja izmaiņas iestādes struktūrā skar Sistēmas drošības vadības organizāciju;

15.1.5. Ja izdarīti grozījumi normatīvajos aktos, kas regulē Sistēmas darbību.

15.2. Ja, pārskatot noteikumus, konstatēta atbilstoša nepieciešamība, tos aktualizēt.