Profesionālās izglītības kompetences centrs
"Rīgas Dizaina un mākslas vidusskola"

K.Valdemāra iela 139, Rīga, LV-1013, tālr. 67360823, e-pasts rdmv@rdmv.lv

IEKŠĒJIE NOTEIKUMI

Rīgā

30.10.2019.

Nr.1-1/14

PAR INFORMĀCIJAS SISTĒMAS DROŠĪBAS POLITIKU

Izdoti saskaņā ar Informācijas tehnoloģiju drošības likumu, Valsts informācijas sistēmu likumu, Fizisko personu datu aizsardzības likumu, 28.07.2015. Ministru kabineta noteikumu Nr.442 „Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" 8.punktu un ievērojot Latvijas standartu LVS ISO/IEC 27001:2013 "Informācijas tehnoloģija. Drošības paņēmieni. Informācijas drošības pārvaldības sistēmas. Prasības"

I VISPĀRĪGIE NOTEIKUMI

1. Iekšējie noteikumi par informācijas sistēmas drošības politiku nosaka kārtību kādā Profesionālās izglītības kompetences centrs "Rīgas Dizaina un mākslas vidusskola", turpmāk tekstā - Iestāde, nodrošina Iestādē izmantotās informācijas sistēmas aizsardzību pret ārējiem un iekšējiem riskiem un nodrošina informācijas sistēmas pieejamību, integritāti un konfidencialitāti saskaņā ar spēkā esošajiem normatīvajiem aktiem.
2. Informācijas sistēmas drošības politika attiecas uz visiem Iestādes Informācijas sistēmas lietotājiem, kuri veic darbības ar informācijas resursiem (piemēram, informācijas sistēmām, informāciju, kas tiek saņemta, apstrādāta, ievadīta, pārsūtīta vai uzglabāta) un tehniskajiem resursiem (piemēram, datoru sistēmām, datoru tīkliem), t.sk.:
   2.1. pilna darba laika, nepilnas slodzes un līgumdarbiniekiem, kuri ir nodarbināti Iestādē;
   2.2. lietotājiem, kuri ir noslēguši līgumu ar Iestādi par datu lietošanu vai kuri uz pieprasījuma pamata saņem datus no Iestādes izmantotām informācijas sistēmām;
   2.3. ārpakalpojumu sniedzējiem vai konsultantiem, kuri strādā Iestādes labā.
3. IT speciālista funkcijas pilnībā vai daļēji var tikt nodotas ārpakalpojumā. Ja tās tiek nodotas daļēji, tad Iestādei ir pienākums parūpēties par pārējo noteikumu ievērošanu citā veidā, piemēram, deleģējot šos pienākumus citam iekšējam darbiniekam. Nododot IT speciālista funkcijas ārpakalpojumā, tiek nodotas arī atbilstošas pilnvaras.
4. Iekšējos noteikumos lietotie termini:

4.1. **Informācijas sistēma** – strukturizēts informācijas tehnoloģiju un datu bāzu kopums, kuru lietojot tiek nodrošināta Iestādes izpildei nepieciešamās informācijas ierosināšana, radīšana, apkopošana, uzkrāšana, apstrādāšana, izmantošana un iznīcināšana.

4.2. **Iestāde** – Iestāde, kas normatīvajos aktos noteiktajā kārtībā organizē un vada informācijas sistēmu darbību.

4.3. **Informācijas sistēmas lietotājs** – persona, kurai ir piešķirtas piekļuves tiesības informācijas sistēmās.

4.4. **IT speciālists** – Iestādes vai ārpakalpojuma darbinieks, kurš Iestādes normatīvajos aktos noteiktā kārtībā veic nepieciešamos datortehnikas apkalpošanas darbus. Ārpakalpojuma gadījumā veicamo darbu apjomu un pienākumus nosaka ārpakalpojuma sniedzēja līguma nosacījumi.

II INFORMĀCIJAS SISTĒMAS DROŠĪBAS POLITIKAS MĒRĶI UN PAMATNOSTĀDNES

5. Iestādes pienākums ir nodrošināt, lai to rīcībā esošā informācija tiktu apstrādāta, glabāta un pārvaldīta droši un pārbaudāmi, sniedzot tās darbiniekiem un lietotājiem skaidri noteiktas prasības informācijas sistēmas iekārtu un resursu izmantošanā, un nodrošinot Informācijas sistēmas aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem apdraudējumiem.
6. Informācijas sistēmas lietotājs, kas ir nodarbināts Iestādē un ir Iestādes darbinieks (pilna darba laika, nepilnas slodzes un līgumdarbiniekiem), atbild par drošības politikas nosacījumu un prasību ievērošanu.
7. Iestādes direktors ir atbildīgs par viņa pakļautībā vai uzraudzībā esošajiem Informācijas sistēmas lietotājiem. Iestādes direktors nodrošina, ka personāls, uz kuru šī politika attiecas daļēji vai pilnā apmērā, ir informēts par politikas esamību un pilda savus darba pienākumus atbilstoši politikas nostādnēm.
   7.1. Informācijas sistēmas drošība tiek nodrošināta šādu mērķu realizācijai:
   7.2. nodrošinātu informācijas pieejamību;
   7.3. nodrošinātu informācijas integritāti;
   7.4. nodrošinātu informācijas konfidencialitāti;
   7.5. aizsargātu sistēmas informācijas resursus;
   7.6. aizsargātu sistēmas tehniskos resursus;
   7.7. noteiktu sistēmas drošības apdraudējumu;
   7.8. novērtētu sistēmas drošības risku;
   7.9. atklātu sistēmas drošības incidentu;
   7.10. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.
8. Iestādē izmantotās informācijas sistēmām ir šādas drošības (pieejamības, integritātes un konfidencialitātes) klases:
   8.1. C pieejamības klase - sistēmas nodrošinātā pakalpojuma neplānots pārtraukums sistēmas paredzētajā darba laikā drīkst būt ilgāks par 24 stundām mēnesī (summāri);
   8.2. B integritātes klase - sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par 24 stundām (summāri) mēnesī, bet tas pieļaujams lielāks par četrām stundām (summāri) mēnesī;
   8.3. A konfidencialitātes klase - sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par četrām stundām

mēnesī (summāri), kā arī sistēmā tiek apstrādāti sensitīvi personas dati vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde var radīt smagākas sekas nekā kaitējums Iestādes, citu Iestādi vai Latvijas Republikas reputācijai.

9. Iestādes būtiskākajās lietošanā esošajās informācijas sistēmās Valsts izglītības informācijas sistēmā (www.viis.lv), Resursu vadības un grāmatvedības programmā "HORIZON", bibliotēku informācijas sistēmā "SKOLU ALISE", Novērtēšanas elektroniskās veidlapas informācijas sistēmā, Kultūras karte (tikai skaitliskā informācija, kas nesatur personas datus) tiek apstrādāti darbinieku personas dati.
10. Iestādes būtiskākajās lietošanā esošajās informācijas sistēmās Valsts izglītības informācijas sistēmā (www.viis.lv), portālā www.e-klase.lv, Resursu vadības un grāmatvedības programmā "HORIZON", bibliotēku informācijas sistēmā "SKOLU ALISE", Kultūras karte (tikai skaitliskā informācija, kas nesatur personas datus) tiek apstrādāti izglītojamo personas dati.
11. Informācijas tehnoloģiju drošības pārvaldību un Informācijas sistēmas drošības politikas koordināciju Iestādē veic IT speciālists.

III INFORMĀCIJAS SISTĒMAS LIETOTĀJU ADMINISTRĒŠANAS KĀRTĪBA

12. Iestādes direktors ir atbildīgs par sev un to padotībā esošo darbinieku Informācijas sistēmas lietotāju pieejas tiesību piešķiršanu, izmaiņu veikšanu un anulēšanu.
13. Pieprasījumus Informācijas sistēmas uzturētājam par Informācijas sistēmas lietotāju pieejas tiesību piešķiršanu vai izmaiņu veikšanu tajos veic Iestādes direktors.
14. Informācijas sistēmas lietotāju pieejas tiesības tiek piešķirtas Iestādes darbiniekiem atbilstoši katra atsevišķā darbinieka noteiktajiem darba pienākumiem un specifikai.
15. Informācijas sistēmas uzturētājs izskata lietotāju pieejas tiesību piešķiršanas pieprasījumu un izveido atbilstošās informācijas sistēmas lietošanas tiesības un nosūta tās Lietotājam.
16. Informācijas sistēmas uzturētājs ir atbildīgs par Lietotāju pieejas tiesību izveidošanu, administrēšanu un šo pieprasījumu apkopošanu, glabāšanu, kontroli un uzraudzību.
17. Piešķirtās lietotāju pieejas tiesības Iestādes informācijas resursiem ir nekavējoties jāanulē šādos gadījumos:
    17.1. darbiniekiem, kuri pārtrauc darba (līguma) tiesiskās attiecības ar Iestādi un / vai tās vairs nav nepieciešamas pienākumu veikšanai;
    17.2. personām, kuras ir izpildījušas savstarpēji noslēgto līgumu ar Iestādi vai šī līguma izbeigšanās (atcelšanas) gadījumā.
18. Iestājoties šo noteikumu 17.punktā minētajam gadījumam, Iestādes direktoram, ir pienākums informēt Informācijas sistēmas uzturētāju, kas veic atbilstošā lietotāja tiesību bloķēšanu.
19. Piešķirtās lietotāju pieejas tiesības var anulēt IT speciālists, balstoties uz atbilstošā lietotāja Informācijas sistēmas drošības politikas vai to saistošo dokumentu pārkāpumiem, par to rakstiski informējot Iestādes direktoru.

IV INFORMĀCIJAS SISTĒMAS LIETOTĀJU TIESĪBAS, PIENĀKUMI UN ATBILDĪBA

20. Informācijas sistēmas lietotājam ir tiesības izmantot viņam lietošanā nodotos datorus un to programmatūru, kā arī Informācijas sistēmas lietotājam ir tiesības pieprasīt atbalstu gadījumā, ja datoram vai tā programmatūrai ir radušies traucējumi.

21. Informācijas sistēmas lietotājs ir atbildīgs par datortehniku, kas nodota viņa rīcībā, kā arī atbild par darbībām, kas tiek veiktas ar viņam nodoto datortehniku.
22. Informācijas sistēmas lietotājs nedrīkst atļaut piekļūt tam nodotai datortehnikai citām personām, ja tas nav nepieciešams tiešo darba pienākumu pildīšanai un to pilnvarojumu nav devis Iestādes direktors vai IT speciālists.
23. Informācijas sistēmas lietotāja pienākums ir apzināti nepieļaut datorvīrusu iekļūšanu iestādes datorsistēmās un neizmantot nezināmas izcelsmes datu nesējus. Rodoties aizdomām, ka dators ir inficēts ar datorvīrusu, par to nekavējoties jāinformē IT speciālists.
24. Informācijas sistēmas lietotājam ir pienākums jebkuru ienākošo elektronisko informāciju (failus) pirms lietošanas obligāti pārbaudīt ar antivīrusa programmatūru, ja tas netiek nodrošināts automātiski.
25. Nelicencētas programmatūras uzstādīšana un lietošana darba stacijās (lietotāja datoros) ir aizliegta. Patvaļīgi uzstādītas programmatūras lietošana, bez Iestādes direktora vai IT speciālista atļaujas ir aizliegta.
26. Informācijas sistēmas lietotājs nedrīkst izpaust nepilnvarotām personām ziņas par Iestādes datoru tīkla uzbūvi un konfigurāciju.
27. Informācijas sistēmas lietotājs nedrīkst no sava darba datora kopēt failus uz ārējiem datu nesējiem (piemēram, CD, DVD, USB kartēm vai citiem datu nesējiem), ja to nevajag tiešo darba pienākumu pildīšanai vai ja tam pilnvarojumu nav devis Iestādes direktors vai IT speciālists.
28. Ārējo datu nesēju, kurā ir iekopēta ierobežotas pieejamības informācija, no Iestādes telpām drīkst iznest tikai ar Iestādes direktora RAKSTISKU atļauju. Šajos gadījumos Informācijas sistēmas lietotājs, kurš no iestādes telpām iznes šādu datu nesēju, uzņemas pilnu materiālo atbildību par šo informāciju un radītajiem zaudējumiem – datu noplūdei.
29. Informācijas sistēmas lietotājam ir aizliegts patvaļīgi pārvietot, demontēt aparatūru, izjaukt, remontēt iekārtas vai veikt citas darbības, kas varētu traucēt informācijas un tehnisko resursu darbību.
30. Informācijas sistēmas lietotājam ir aizliegts veikt paroļu minēšanu, drošības ievainojamības pārbaudes, kodēto datu atkodēšanu, izmantot noklausīšanās programmas un veikt citas darbības, kas vērstas uz informācijas un tehnisko resursu drošības vājināšanu.

V INTERNETA UN E-PASTA LIETOŠANA

31. Pieeju Internetam darbiniekiem piešķir vienlaicīgi ar Informācijas sistēmas lietotāja pieejas tiesībām Iestādes datortīklam (domēnam), kas nepieciešams, lai nodrošinātu iestādes darbību un klientiem sniegtos pakalpojumus.
32. Informācijas sistēmas lietotājam darba vajadzībām ir jāizmanto tikai Iestādes piešķirtais e-pasts.
33. Informācijas sistēmas lietotājam ir aizliegts, izmantojot Iestādes piešķirto e-pastu, reģistrēties dažādos interneta resursos, kas tiek izmantoti privātām vajadzībām.
34. Informācijas sistēmas lietotājam ir aizliegts atvērt e-pasta pielikumus vai atvērt sūtījumā iekļautās Interneta adreses, kas saņemtas no nenoskaidrotiem sūtītājiem.
35. Lietojot Internetu, darbinieki pārstāv Iestādi un tie ir atbildīgi, lai Internets tiktu izmantots darba vajadzībām ētiski un atbilstoši normatīvo aktu prasībām.
36. Darbiniekiem, izmantojot e-pastu, ir jānodrošina, ka visas komunikācijas tiek veiktas profesionālām vajadzībām un netraucē pašu darbinieku darba produktivitāti, kā arī netiek izplatīta vai sūtīta informācija, kas ir aizsargāta ar autortiesībām. Iestāde no darbinieka ir

tiesīga piedzīt zaudējumus, kas Iestādei var būt radušies, maksājot atlīdzību autortiesību īpašniekam par autortiesību pārkāpumu.

37. Darbinieki ir atbildīgi par visu nosūtīto tekstuālo, audio un vizuālo saturu. IT speciālists bez saskaņošanas ar darbinieku patur sev tiesības pārlūkot darbinieku saņemto un nosūtīto e-pastu saturu, ja uzskata to par nepieciešamu.
38. IT speciālistam ir tiesības bloķēt atsevišķu interneta resursu izmantošanu, kā arī ir tiesības piekļūt Informācijas sistēmas lietotāja saglabātajai informācijai, kas atrodas uz Informācijas sistēmas lietotāja datoriem vai serveriem, tikai pildot amata pienākumus vai pildot direktora rīkojumus.
39. Darbiniekiem ir aizliegts sūtīt tā sauktās "ķēdes vēstules" (t.sk. mēstules, reklāmas, aģitācijas un tml.) – elektroniskus ziņojumus ar lūgumu pārsūtīt tos citiem adresātiem, kā arī ir aizliegts atvērt un darbināt no Interneta tīkla saņemtus aizdomīgus failus. Informācijas sistēmas lietotājam ir jāatceras, ka Interneta tīkls nav drošs datu pārraides mēdijs un nosūtītāja identifikāciju var viegli viltot. Ja par failu rodas šaubas, Informācijas sistēmas lietotājam ir nepieciešams sazināties ar nosūtītāju un noskaidrot, vai šāds dokuments ir ticis nosūtīts.
40. Darbinieki ārpus Iestādes nedrīkst sūtīt e-pastu vairākiem adresātiem vienlaicīgi, atklājot visu saņēmēju e-pasta adreses, ja tajās ir iekļauts personas vārds un uzvārds. Ja sūta e-pastu vairākiem adresātiem vienlaicīgi, tad izmantot diskrēto kopiju lauku (Bcc), nevis (Cc) lauku, kas saņēmējiem paslēpj visas (Bcc) laukā norādītās e-pasta adreses.

VI INFORMĀCIJAS SISTĒMAS LIETOTĀJA PIEEJAS PAROLES UZBŪVE UN LIETOŠANA

41. Iestādes informācijas resursu aizsardzība tiek nodrošināta ar datora paroli datortīkla (domēna) līmenī, kam ir jāatbilst vismaz sekojošām prasībām:
    41.1. minimālam paroles garumam ir jābūt vismaz 9 simboliem;
    41.2. maksimālais paroles maiņas periods nedrīkst būt ilgāks par 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā;
    41.3. paroles uzbūvei jābūt komplicētai, izmantojot vismaz vienu lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un īpašo rakstzīmju kombināciju (kā piemēram, !@#$%^*()_+);
    41.4. izveidojot paroli, tā nedrīkst sakrist ar nevienu no 5 iepriekšējām parolēm;
    41.5. Informācijas sistēmas lietotāja parole pie ievades nedrīkst parādīties uz ekrāna.
42. Informācijas sistēmas lietotājs nedrīkst izpaust savu paroli jebkurām citām trešajām personām vai citiem lietotājiem, izņemot atsevišķos gadījumos savas prombūtnes laikā, ja atļauju ir devis Iestādes direktors.
43. Informācijas sistēmas lietotājs nedrīkst savu paroli pierakstīt uz papīra, ja šo dokumentu neglabā seifā vai citā vietā ar ierobežotu citu personu piekļuvi.
44. Ja Informācijas sistēmas lietotājam rodas aizdomas, ka viņa paroli ir uzzinājusi jebkura cita persona, Informācijas sistēmas lietotājam ir pienākums pēc iespējas īsākā laikā šo paroli nomainīt patstāvīgi vai lūgt IT speciālistu to izdarīt savā vietā.
45. Informācijas sistēmas lietotājs ir atbildīgs par informācijas aizsardzību un tā pienākums ir nodrošināt, ka datoriem Informācijas sistēmas lietotāja prombūtnes laikā ir ieslēgts ar paroli aizsargāts ekrānsaudzētājs vai noslēgta datora darbvirsma ar Windows + L taustiņu kombināciju.

46. Dienas beigās, beidzot darbu pie datora, tas jāizslēdz izmantojot procedūru: Start => Shut Down => Ok.

VII INFORMĀCIJAS SISTĒMAS DROŠĪBAS ORGANIZĀCIJA

47. Informācijas sistēmas drošības organizatoriskās struktūras pamatu veido IT speciālists un Informācijas sistēmas lietotāji.
48. IT speciālists nodrošina informācijas sistēmas drošības politikas realizāciju, kā arī veic šādas darbības:
    48.1. aktualizē drošības politiku, izstrādā ar informācijas sistēmas drošības saistīto iekšējo normatīvo aktu projektus un veic tās koordināciju;
    48.2. aktualizē Informācijas sistēmas drošības politiku un to saistītos dokumentus vismaz vienu reizi gadā, kā arī šādos gadījumos:
        48.2.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;
        48.2.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;
        48.2.3. ja pēkšņi pieaug sistēmas drošības incidentu skaits vai ir noticis nozīmīgs sistēmas drošības incidents;
        48.2.4. ja izmaiņas Iestādes organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;
        48.2.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.
    48.3. nodrošina informācijas sistēmās izmantojamās informācijas racionālu un pareizu izmantošanu;
    48.4. izskata informācijas sistēmas lietotāju tiesību piešķiršanas un izmaiņu veikšanas pieteikumu autorizāciju saskaņā ar Informācijas sistēmas lietošanas noteikumiem;
    48.5. piedalās Risku vadības procesā saskaņā ar Informācijas sistēmu drošības riska pārvaldības plānu;
    48.6. nodrošina atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši šīs politikas prasībām;
    48.7. Iestādes direktors IT speciālista prombūtnes gadījumā ieceļ tā pienākumu aizvietotāju.
49. IT speciālista pienākums ir:
    49.1. nodrošināt tehnisko resursu racionālu un pareizu izmantošanu;
    49.2. nodrošināt tehnisko resursu fiziskās un loģiskās aizsardzības pasākumus saskaņā ar Informācijas sistēmas drošības noteikumiem;
    49.3. veikt nepieciešamo tehnisko risinājumu uzstādīšanu un konfigurēšanu;
    49.4. veikt risku vadības procesa koordināciju Iestādē saskaņā ar Informācijas drošības riska pārvaldības plānu;
    49.5. izmeklēt informācijas drošības incidentus;
    49.6. veikt regulāras pārbaudes, lai pārliecinātos, ka tiek ievērotas Informācijas sistēmas drošības politikas un to saistošo dokumentu prasības;
    49.7. nodrošināt informācijas sistēmas atjaunošanas procedūras, ja tehnoloģiskie resursi ir bojāti un informācijas sistēmas funkcionēšana traucēta vai neiespējama saskaņā ar Informācijas sistēmas drošības noteikumiem un Informācijas sistēmu atjaunošanas plānu;
    49.8. pēc Iestādes direktora pieprasījuma, sagatavot Lietotāju pieejas tiesību sarakstu.

49.9. nodrošināt atbilstošu atbalstu, palīdzību un konsultāciju sniegšanu personālam, lai tas varētu pildīt savus pienākumus atbilstoši Informācijas sistēmas drošības politikas prasībām.

50. Informācijas sistēmas lietotāja pienākums ir racionāli un lietderīgi izmantot informācijas sistēmas un to datus sava darbu pienākumu veikšanai.

VIII INFORMĀCIJAS RESURSU KLASIFIKĀCIJA

51. Visiem Iestādes informācijas resursiem (t.sk., darba stacijām, serveriem, perifērijas iekārtām, programmatūrai, Informācijas sistēmas datiem) ir jābūt uzskaitītiem un reģistrētiem, kā arī Informācijas sistēmas datiem ir jābūt klasificētiem.
52. Iestādes informācijas resursu klasificēšana tiek veikta atbilstoši Informācijas atklātības likumam un iekšējiem noteikumiem par ierobežotas pieeejamības informācijas sarakstu.

IX INFORMĀCIJAS RESURSU RISKA ANALĪZE

53. Informācijas resursu riska analīzes mērķis ir nodrošināt atbilstošu Informācijas sistēmas vadību un kontroles sistēmas darbības efektivitāti, lai atklātu un novērstu kļūdas un neprecizitātes, un nepieciešamības gadījumā veiktu labojumus drošības sistēmā.
54. Iestādes informācijas resursu riska analīze tiek veikta atbilstoši Informācijas sistēmas drošības riska pārvaldības plānam (skatīt 1. pielikumu).

X INFORMĀCIJAS LOĢISKĀ AIZSARDZĪBA

55. Iestādes datortīklu, datoru un to saistīto iekārtu uzturēšanu un administrēšanu, kā arī Informācijas sistēmas lietotāju datoru uzstādīšanu un administrēšanu veic IT speciālists.
56. IT speciālists ir atbildīgs par piemērotu un efektīvu aizsardzības sistēmas izveidi, lietojot atbilstošu maršrutēšanas un ugunsmūra sistēmu, kā arī nodrošinot pretvīrusu programmatūras uzstādīšanu un uzturēšanu uz Iestādes datoriem.
57. IT speciālistam ir pienākums regulāri sekot līdzi ugunsmūra paziņojumiem un reaģēt uz vīrusu uzbrukumiem, nodrošinot konstatēto vīrusu iznīcināšanu un būtisko incidentu reģistrēšanu.
58. Gadījumā, ja tiek konstatēti ielaušanās mēģinājumi vai būtiski incidenti, IT speciālists veic to reģistrēšanu un izmeklēšanu, kā arī par tās rezultātiem informē Informācijas tehnoloģiju drošības incidentu novēršanas institūcijā pa talruni +37167085888 (ziņojumu pieņemšana visu dienakti) E-pasts: cert@cert.lv vai cert@cert.gov.lv
59. Vīrusu darbības novēršanai veic šādus pasākumus:
    59.1. IT speciālists veic pasākumus datoru vīrusu darbības novēršanai tehniskajos resursos, izmantojot šim nolūkam paredzētu programmatūru;
    59.2. IT speciālists veic antivīrusu programmu pārraudzību, lai pārliecinātos par to darbību un jaunāko vīrusu definīciju failu esamību.
60. IT speciālists izveido, veic izmaiņas un anulē Informācijas sistēmas lietotāju tiesības pēc direktora pieprasījuma.
61. Informācijas sistēmas lietotājiem, kuri ir Iestādes darbinieki, autorizēšanās rekvizītus (lietotājvārdu un paroli) izsniedz IT speciālists vai arī atbilstošās informācijas sistēmas pakalpojumu sniedzējs.

62. Informācijas sistēmas lietotājiem, kuri nav Iestādes darbinieki, autorizēšanās rekvizītus neizsniedz.
63. Ja Informācijas sistēmas lietotājs, kas ir Iestādes darbinieks, ir aizmirsis savu lietotāja paroli, par to Informācijas sistēmas lietotājs personīgi vai telefoniski informē IT speciālistu vai ārpakalpojumu sniedzēju. IT speciālists vai ārpakalpojumu sniedzējs identificē atbilstošo informācijas sistēmas lietotāju, izveido jaunu paroli un izsniedz atbilstošajam Informācijas sistēmas lietotājam.
64. IT speciālists vai atbilstošās informācijas sistēmas pakalpojumu sniedzējs nodrošina auditācijas pierakstu veidošanu par informācijas sistēmām, kas ir izvietotas uz Iestādes resursiem vai kuras ir Iestādes īpašumā. Auditācijas pierakstos iekļauj visus veiksmīgus un neveiksmīgus pieslēgšanās gadījumus, to datumus un laiku, kā arī šo lietotāju (t.sk. administratora) vārdus vai citu autentifikācijas līdzekli. IT speciālists nodrošina auditācijas pierakstu integritāti un regulāri veido auditācijas pierakstu datu rezerves kopijas. Par datortīkla auditācijas pierakstu veidošanu atbildīgs ir IT speciālists.
65. Atbilstošās informācijas sistēmas pakalpojumu sniedzējs nodrošina, ka pirms jaunas sistēmas pieņemšanas ekspluatācijā tai ir veikti ielaušanās testi. Ielaušanās testus veic juridiska persona vai Iestādes darbinieki, kuri nav piedalījušies sistēmas izstrādē.
66. IT speciālists veic auditācijas pierakstu analīzi šādos gadījumos:
    66.1. Informācijas sistēmas lietotāja atkārtota neveiksmīga pieslēgšanās informācijas sistēmai;
    66.2. Informācijas sistēmas lietotāja pieslēgšanās informācijas sistēmai ārpus darba laika;
    66.3. mēģinājumi piekļūt informācijas resursiem, kuriem IT speciālists nav pilnvarojis piekļūt;
    66.4. atkārtoti mēģinājumi lietot lietotāja rekvizītus, kuri jau ir atcelti;
    66.5. nesankcionētas programmatūras konfigurācijas maiņas un neatļautas programmatūras uzstādīšana.
67. IT speciālistam ir pienākums informēt Iestādes vadību par programmatūras licencēm, kurām tuvākā mēneša laikā beigsies termiņš un pēc nepieciešamības sniegt arī priekšlikumus un konsultācijas saistībā ar jaunas programmatūras iegādi.
68. Reģistru par iegādātiem un uzstādītiem informācijas tehniskajiem resursiem (t.sk. par darba stacijām, serveriem un perifērijas iekārtām) veic Iestādes grāmatvedība. Vismaz reizi gadā tiek veikta šo resursu inventarizācija, pārliecinoties, ka šis reģistrs ir korekts.
69. IT speciālists, tā pilnvarota persona vai ārējs konsultants nodrošina Iestādes Informācijas sistēmas lietotāju apmācību informācijas sistēmu drošības jomā, izskaidrojot tiem Informācijas sistēmas drošības politikas pamatprincipus un būtiskākos drošības pasākumus datu drošībai.
70. Iestādē tiek nodrošināta datortīkla / informācijas sistēmas atbilstība šādām aizsardzības prasībām:
    70.1. iekšējo datortīklu nodala no interneta ar ugunsmūra palīdzību;
    70.2. ja tehniskais risinājums to pieļauj, nodrošina datortīkla / informācijas sistēmas pretvīrusa aizsardzību;
    70.3. nodrošina nepārtrauktu datortīkla / informācijas sistēmas darba vides drošības apdraudējumu novēršanu, izmantojot ielaušanās mēģinājumu noteikšanu un aizsardzības sistēmu;

70.4. izmantojot tikai šifrētu pieslēgumu un ja iespējams, tad daudzfaktoru autentifikāciju, nodrošina attālinātas piekļuves ierobežošanu datortīkla / informācijas sistēmas administrēšanai;

70.5. sistēmu testēšanai organizē uz servera loģiskā vai fiziskā līmenī individuāli nodalītu testēšanas vidi;

70.6. piekļuvi datortīkla / informācijas sistēmas administrēšanas un pārvaldības funkcionalitātei nodrošina tikai tām personām, kurām datortīkla / informācijas sistēmas esošā informācija atbilstošā apmērā ir nepieciešama darba pienākumu veikšanai;

70.7. sistēmas lietotāji, kas veic sistēmas administrēšanas darbu, izmanto īpašus lietotāju kontus (piemēram, sistēmas administratora konts), kas netiek izmantoti ikdienas darbību veikšanai;

70.8. sistēmās vēlams nodrošināt, lai katrs lietotāja konts ir saistīts ar konkrētu fizisko personu. Ja sistēmā tiek izmantoti konti, kas nav piesaistāmi konkrētai fiziskai personai, tad sistēmā jābūt iestrādātiem tehniskiem līdzekļiem, kas novērš iespēju lietotājiem izmantot šādus kontus;

70.9. sistēmas lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros;

70.10. sistēmas lietotāja parole ievadīšanas brīdī lietotājam netiek pilnībā attēlota;

70.11. sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir lietojama vienu reizi un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;

70.12. sistēmā nav pieļaujama funkcionalitāte, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;

70.13. iekārtām, tai skaitā infrastruktūras iekārtām, kas nodrošina sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;

70.14. tiek nodrošināta sistēmas auditācijas pierakstu (turpmāk – sistēmas pieraksti) veidošana un uzglabāšana vismaz sešus mēnešus pēc ieraksta izdarīšanas;

70.15. jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola (IP) adresei;

70.16. sistēmai jābūt uzliktiem visiem pieejamiem programmatūras atjauninājumiem, iepriekš izvērtējot to nepieciešamību;

70.17. visās Iestādes valdījumā esošajās galalietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, jābūt iekļautai pretvīrusu funkcionalitātei;

70.18. sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām;

70.19. piecas secīgas reizes nepareizi ievadot sistēmas lietotāja konta paroli, šis konts (izņemot sistēmas administratora kontu) nekavējoties tiek bloķēts;

70.20. ar sistēmas administratora kontu piekļūt sistēmai, izmantojot iekārtas, kas atrodas ārpus Iestādes telpām, kā arī iekārtas, kas neatrodas Iestādes valdījumā, iespējams, tikai izmantojot daudzfaktoru autentifikāciju;

70.21. fiziski piekļūt iekārtām, kas nodrošina sistēmas darbību, atļauts vienīgi Iestādes pilnvarotām personām;

70.22. Iestādes iekšēji izstrādātajām sistēmām lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu;

70.23. plūsma starp sistēmu un tās lietotājiem, kā arī starp sistēmu un citām sistēmām tiek kontrolēta, piemēram, izmantojot ugunsmūri;

70.24. datortīkla pakalpojumi, kas netiek izmantoti sistēmas darbības nodrošināšanai, ir atslēgti;

70.25. veicot sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu sistēmā glabāto datu integritātei;

70.26. sistēmas izvietošana ārpakalpojuma sniedzēja nodrošinātos resursos atļauta tikai tad, ja pakalpojuma 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.

71. Iestāde nodrošina, ka vismaz reizi gadā tiek veikta informācijas tehnoloģiju drošības pārbaude (t.i. Iestādes izmantotās informācijas sistēmas drošības dokumentācijas un pasākumu atbilstības pārbaude) un atbilstoši tās rezultātiem tiek organizēta atklāto trūkumu novēršana.

72. Iestāde nodrošina, ka vismaz reizi gadā IT speciālists apmeklē Drošības incidentu novēršanas institūcijas organizētu apmācību informācijas tehnoloģiju drošības jautājumos.

73. Iestāde nodrošina, ka ne retāk kā reizi gadā veikt institūcijas darbinieku instruktāžu informācijas tehnoloģiju drošības jautājumos.

74. Datu nesēju (t.sk. CD, DVD, USB Flash, ārējais cietais disks vai tml.) fizisko aizsardzību nodrošina katrs Informācijas sistēmas lietotājs, nodrošinot, ka tie tiek glabāti drošās vietās, lai novērstu jebkādu nepilnvaroto personu piekļuvi

XI DARBĪBAS NEPĀRTRAUKTĪBAS NODROŠINĀŠANA

75. Iestādes informācijas sistēmām un elektroniskā veidā saglabātai informācijai regulāras rezerves kopijas veidošanu nodrošina IT speciālists atbilstoši Informācijas sistēmas drošības noteikumiem.

76. Katram Informācijas sistēmas lietotājam, kas ir nodarbināts Iestādē, ir jāveic un jānodrošina darbības nepārtrauktību tādā apjomā, kādā tā ir noteikta konkrētā darbinieka pienākumos un cik tas nepieciešams darbinieka tiešajiem darba pienākumiem.

77. Par visām avārijas situācijām (t.sk. ugunsgrēku, plūdiem, nelaimes gadījumiem utt.) Informācijas sistēmas lietotājiem un IT speciālistam ir nekavējoši jāpaziņo Iestādes direktoram.

XII ĀRPAKALPOJUMU IESAISTE

78. Ja Iestādes sistēmas uzturēšanai slēdz ārpakalpojuma līgumu ar pakalpojuma sniedzēju, līguma izpildi uzrauga atbildīgā persona un līgumā iekļauj vismaz šādas drošības prasības:

78.1. saņemamā ārpakalpojuma aprakstu;

78.2. precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;

78.3. Iestādes un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā:

78.3.1. Iestādes tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi;

78.3.2. Iestādes tiesības iesniegt ārpakalpojuma sniedzējam pamatotu rakstisku pieprasījumu nekavējoties izbeigt ārpakalpojuma līgumu, ja Iestāde konstatējusi,

ka ārpakalpojumu sniedzējs nepilda ārpakalpojuma līgumā noteiktās prasības attiecībā uz ārpakalpojuma apjomu vai kvalitāti;

78.3.3. ārpakalpojuma sniedzēja pienākumu nodrošināt Iestādei iespēju pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti;

78.3.4. iekļaujot pušu atbildību, atbilstoši jaunās datu regulas prasībām, nodrošinot, ka datu saņēmējs/uzglabātājs uzņemas pilnu atbildību par personu datu drošību un apstrādi;

78.3.5. nepieciešamās izmaiņas lietotāju kontos piesakāmas tikai caur vienu atbildīgo personu.

79. Ja Iestāde uzsāk iepirkumu par esošas ārpakalpojumu sistēmas uzlabojumiem vai iegādi, tas nodrošina, ka iepriekš minētās ārpakalpojumu iesaistes drošības prasības tiek iekļautas iepirkuma specifikācijā.

80. Ja Iestāde uzsāk iepirkumu par jaunas sistēmas izstrādi, tā iepirkuma specifikācijā iekļauj prasības, paredzot:

80.1. noteiktu sistēmas uzturēšanas un atbalsta nodrošināšanas (tai skaitā sistēmas drošības nepilnību novēršanas) laikposmu;

80.2. sistēmas datorprogrammu pirmkoda un tā izmantošanas tiesību nodošanu Iestādesm ne vēlāk kā pēc noteiktā laikposma beigām, kā arī pēc katru izmaiņu vai uzlabojumu veikšanas tajā;

80.3. iespēju noteiktajā laikposmā turpināt sistēmas ekspluatēšanu ar sistēmas funkcionēšanai obligāti nepieciešamā programmnodrošinājuma (piemēram, operētājsistēma, datubāzu vadības sistēma, interpretators) jaunākām versijām.

XIII REZERVES KOPIJU VEIDOŠANAS KĀRTĪBA

81. Informācijas sistēmas nodrošinātājs nodrošina Iestādes informācijas resursu rezerves kopiju veidošanu informācijas sistēmām.

82. Citiem informācijas resursiem, kas ir izvietoti uz Iestādes datoriem vai datu nesejiem, atbild darbinieks, kas šo informāciju lieto.

83. Rezerves kopiju ārējos datu nesējus glabā attālināti no oriģinālajiem datiem, lai novērstu oriģināla un kopijas vienlaicīgas bojāejas iespēju liela apjoma negadījuma situācijā.

84. Iestādes direktors nosaka vietu, kur tiks glabātas rezerves kopijas uz ārējā datu nesēja.

85. IT speciālists nodrošina Iestādes informācijas resursu atjaunošanu no rezerves kopijām.

86. IT speciālistam ir pienākums vismaz reizi gadā veikt pārbaudi par informācijas sistēmu atjaunošanas iespējām no rezerves kopijām.

XIV ELEKTRONISKO DATU NESĒJU IZNĪCINĀŠANAS PROCEDŪRA

87. Iestādes darbinieki datu nesējus, kuri satur fiziskas personas datus un kuri paredzēti iznīcināšanai, nogādā IT speciālistam. IT speciālists nodrošina minēto datu nesēju drošu iznīcināšanu šādā kārtībā:

87.1. CD, Blue Ray vai DVD matricas tiek iznīcinātas speciālā griezējā, sasmalcinot tos tā, ka nav iespējams atjaunot;

87.2. USB un SD atmiņu kartes atkārtotai lietošanai tiek pārrakstītas ar „0" un „1", vai - ar defektiem - tiek fiziski iznīcinātas;

87.3. Datoru cietie diski (gan iekšējie, gan ārējie) tiek formatēti un pēc tam pārrakstīti ar „0" un „1" vai - ar defektiem - tiek fiziski iznīcināti.

XV DARBĪBAS TRAUCĒJUMA IDENTIFICĒŠANA

88. Īslaicīgs informācijas sistēmas darbības traucējums ir situācija, kas atbilst šādiem nosacījumiem:
    88.1. pārtraukta vai daļēji pārtraukta informācijas sistēmas darbība, kas nepārsniedz 2 (divas) stundas;
    88.2. identificējot šo traucējumu, IT speciālistam ir saprotami darbības traucējuma iemesli un ir pamatota pārliecība, ka šis traucējums tiks novērsts 2 (divu) stundu laikā.
89. Ilglaicīgs darbības traucējums ir situācija, kas atbilst šādiem nosacījumiem:
    89.1. pārtraukta vai daļēji pārtraukta informācijas sistēmas darbība, kas pārsniedz 2 (divas) stundas;
    89.2. identificējot šo traucējumu, IT speciālistam ir saprotami darbības traucējumu iemesli, apzinoties, ka to novēršanai būs nepieciešams laiks ilgāks par 2 (divām) stundām.
90. Informācijas sistēmas darbības traucējums var rasties, ja:
    91. ir pilnīgi vai daļēji pārtraukta Iestādes pakalpojumu sniegšana;
    92. ir konstatēts, ka pakalpojumu sniegšanu nevar atjaunot nepieciešamajā apjomā un kvalitātē.

XVI DARBĪBAS TRAUCĒJUMA NOVĒRŠANA

93. Pēc darbības traucējuma atklāšanas pirmais uzdevums ir noteikt, vai situācijas bīstamības līmenis prasa personāla evakuāciju. Ja radusies situācija, kā rezultātā izraisīti būtiski ēku un iekārtu bojājumi, situāciju konstatējušajam Iestādes darbiniekam nekavējoties jāinformē direktors un IT speciālists.
94. IT speciālists pēc darbības traucējuma identificēšanas pārņem situācijas vadību un informē par darbības traucējumu iesaistītos Iestādes darbiniekus.
95. Rīcība atsevišķos ārkārtas situāciju gadījumos un turpmāko bojājumu novēršanā:
    95.1. ugunsgrēka trauksmes, atklātas uguns vai piedūmojuma gadījumā jārīkojas atbilstoši „Rīcības plāns ugunsgrēka gadījumā". Ugunsgrēka gadījumā nekavējoties zvanīt 112;
    95.2. elektrības padeves pārrāvumu gadījumā, pazūdot apgaismojumam (būtiski telpām bez āra apgaismojuma piekļuves vai diennakts tumšajā laikā), jāatstāj darba vietu;
    95.3. serveri elektroapgādes traucējumu gadījumiem ir pieslēgti pie nepārtrauktās barošanas avotiem.
    95.4. ilgstošu elektroapgādes pārtraukumu gadījumā IT speciālists dod nepieciešamos rīkojumus par turpmākajām darbībām.
96. Seku novēršanas un atjaunošanas grupā iekļauj IT speciālistu un/vai darbiniekus.
97. Negadījumu seku novēršanas un atjaunošanas grupas pienākumi:
    97.1. pieņemt lēmumu par konkrētām reaģējošām darbībām negadījumu seku novēršanai;
    97.2. novērtēt darbinieku apdraudējumu, telpu un iekārtu bojājumu pakāpi un stāvokli;
    97.3. identificēt un novērtēt bojātās sistēmas nozīmīgumu Iestādes darbībai, noteikt apdraudējuma vai darbības pārtraukuma iemeslus;

97.4. novērtēt Iestādes radītos zaudējumus infrastruktūras un informācijas sistēmu atjaunošanai;

97.5. noteikt apdraudēto vai skarto teritoriju. Pieņemt lēmumu par darbības atjaunošanu esošajās telpās vai pārvietot to uz citām telpām;

97.6. noteikt turpmākās darbības sistēmas atjaunošanai, to prioritāro kārtību, nepieciešamās darbības datu bāžu vai atsevišķu failu atjaunošanai, kā arī noteikt paredzamo darbības atjaunošanai nepieciešamo laiku;

97.7. sadarbībā ar IT speciālistu sastādīt aizvietošanai nepieciešamā aprīkojuma sarakstu (aparatūra, programmatūra, palīgmateriāli).

98. IT speciālistam ir pienākums nodrošināt iesaistītiem darbiniekiem atbilstošas apmācības informācijas sistēmu darbības nepārtrauktības nodrošināšanai.

Direktors Alvis Līdaks

Datu aizsardzības speciālists
Dagnija Baldiņa
Dagnija.Baldina@inbox.lv

1.pielikums
Informācijas sistēmas drošības riska pārvaldības plans

I Informācijas resursu risku identificēšana

1. Risku pārvaldnieks ir iestādes vai ārpakalpojuma darbinieks, kurš iestādes normatīvajos aktos noteiktā kārtībā veic IT risku pārvaldību. Ārpakalpojuma gadījumā veicamo darbu apjomu un pienākumus nosaka ārpakalpojuma sniedzēja līguma nosacījumi. Risku pārvaldnieks kopīgā sanāksmē ar pieaicinātiem dalībniekiem, ņemot vērā kopējo dalībnieku kompetenci, zināšanas un pieredzi, veic Iestādes funkciju un uzdevumu izpildes procesa posmu izskatīšanu, identificējot tajos iespējamos informācijas resursu riskus. Risku vadības procesa koordināciju un metodisko vadību veic Risku pārvaldnieks.
2. Iestādes informācijas risku analīze tiek veikta pēc sekojošiem soļiem hronoloģiskā secībā:
   3.1. risku identificēšana;
   3.2. risku novērtēšana;
   3.3. risku vadīšana;
   3.4. risku uzraudzība.
3. Risku pārvaldniekam ir pienākums augstāk minētās sanāksmes laikā apkopot identificētos informāciju resursu riskus, iekļaujot tos Risku reģistrā.
4. Lietotājiem ir pienākums ziņot Risku pārvaldniekam par potenciālajiem apdraudējumiem, ievainojamībām, incidentiem, riskiem un to ietekmi.
5. Risku pārvaldnieks risku analīzi veic ikreiz, kad tiek ieviestas būtiskas izmaiņas, kas attiecas uz informācijas sistēmu, turpmāk tekstā- IS, drošību, kā arī uzsākot katru IS informācijas un tehnisko resursu izstrādes, iegādes vai izmaiņu veikšanas projektu.
6. Risku pārvaldnieks katru no identificētajiem riskiem kategorizē, piešķir tam unikālu identifikatoru, kā arī veic tā iestāšanās varbūtības un ietekmes uz Iestādes IS drošību novērtējumu.
7. Riska iestāšanās varbūtība ir iespējamais tā iestāšanās biežums viena kalendārā gada laikā, kas tiek noteikts balstoties uz vēsturisko Iestādes rīcībā esošo informāciju par notikušajiem drošības incidentiem, ņemot vērā industrijas labās prakses norādes un vadlīnijas attiecībā uz konkrētu risku novērtēšanu, kā arī balstoties uz citu Iestādes rīcībā esošo informāciju, kas ļauj iegūt objektīvu novērtējumu attiecībā uz konkrēto risku.
8. Riska iestāšanās varbūtību un ietekmi novērtē trīs līmeņos, katram no tiem piešķirot novērtējumu skaitliskā izteiksmē:
9. Riska iestāšanās varbūtība:

9.1. Zems līmenis (0-30%);
9.2. Vidējs līmenis (31-70%);
9.3. Augsts līmenis (71-100%).

10. Riska iestāšanās gadījumā tā potenciālo seku ietekme:

Notikums/Riska līmenis	**Zems līmenis**	**Vidējs līmenis**	**Augsts līmenis**
Zaudējumi materiālā izteiksmē bez PVN	Iestādei nodarītie finanšu zaudējumi nepārsniegs EUR 1000.00.	Iestādei nodarītie finanšu zaudējumi būs robežās no EUR 1000.00 līdz 5000.00	Iestādei nodarītie finanšu zaudējumi pārsniegs EUR 5000.00.

Ietekme IS datu integritāti	īslaicīga ietekme uz iestādes pamata darbības funkciju izpildes nodrošināšanu vai pamata drošības IS funkcionalitāti	negatīvi ietekmēta pamata drošības IS datu integritāte	negatīvi ietekmēta paaugstinātas drošības IS datu integritāte
ierobežotas pieejamības informācija		ierobežotas pieejamības informācija, kas nesatur fizisku personu sensitīvus datus, nonāks citu juridisku vai fizisku personu rīcībā	ierobežotas pieejamības informācija, kas satur fizisku personu sensitīvus datus, nonāks citu juridisku vai fizisku personu rīcībā
pamata drošības IS pārrāvuma ilgums	tiks apturēta viena vai vairākas iestādes pamata drošības IS uz laiku līdz 8 h.	tiks apturēta viena vai vairākas iestādes pamata drošības IS uz 8-24 h	tiks apturēta viena vai vairākas iestādes pamata drošības IS uz vairāk kā 24 h
paaugstinātas drošības IS pārrāvuma ilgums		tiks apturēta viena vai vairākas iestādes paaugstinātas drošības IS uz 1h-8h	tiks apturēta viena vai vairākas iestādes paaugstinātas drošības IS uz vairāk kā 8 h

11. Riska iestāšanās varbūtības un atstātās ietekmes līmeņa noteikšanu uz Iestādes darbību veic Risku pārvaldnieks, kurš vērtējuma sagatavošanas laikā, lai nodrošinātu iespējami pilnvērtīgākā vērtējuma veikšanu, var piesaistīt citus Iestādes nodarbinātos, atbilstoši to kompetencē esošajiem darbības jautājumiem, kā arī trešo pušu pārstāvjus atzinumu un ieteikumu sniegšanai attiecībā uz konkrētiem riskiem
12. Riska iestāšanās varbūtības un atstātās ietekmes līmeņa noteikšanas iedalījums:

Ietekme \Varbūtība	**3 – Augsta**	**2 – Vidēja**	**1 – Zema**
3 – Augsta	9 –Augsta	6 – Augsta	3 – Vidēja
2 – Vidēja	6 – Augsta	4 – Vidēja	2 – Zema
1 – Zema	3 – Vidēja	2 – Zema	1 – Zema

13. Pēc katra riska iestāšanās varbūtības un ietekmes līmeņa noteikšanas, nosaka kopējo riska līmeni, kuru veido iestāšanas **varbūtības un ietekmes kritēriju reizinājums,** ko novērtē šādi:
13.1. augsts riska līmenis (novērtējums ir 6 vai 9) - viens no riska novēršanas kritērijiem ir vērtēts kā augsts, bet otrs kā vidējs vai abi kritēriji ir vērtēti kā augsti;
13.2. vidējs riska līmenis (novērtējums diapazonā no 3 līdz 4) – viens no riska novērtēšanas kritērijiem ir vērtēts kā augsts, bet otrs kā zems vai arī abi kritēriji ir vērtēti kā vidēji;

13.3. zems riska līmenis (novērtējums ir 1 vai 2) – viens no riska novēršanas kritērijiem ir vērtēts kā vidējs, bet otrs kā zems.

14. Ne retāk kā reizi gadā, IT speciālists veic visaptverošu IS drošības risku analīzi, kuras ietvaros tiek apskatīti jau iepriekš identificētie riski un veiktie pasākumi risku mazināšanai kā arī apzināti jauni, iepriekš vēl neidentificēti, riski. Risku analīzes rezultātā IT speciālists sagatavo ziņojumu, kurā iekļauj vismaz sekojošo informāciju:

14.1. Apkopojumu par gada laikā identificētajiem riskiem pamatojoties uz risku reģistru;

14.2. Risku pārvaldības plānu.

15. Informācijas resursu risku reģistra paraugs

INFORMĀCIJAS RESURSU RISKU REĢISTRS

Riska Nr.	Informācijas resursu risku nosaukums (raksturojums)	Varbūtība	Ietekme	Pārvaldība	Risku rādītājs
1.					
2.					
3.					

16. Pārskata par pasākumiem risku mazināšanai un novēršanai paraugs

PĀRSKATS PAR PASĀKUMIEM RISKU MAZINĀŠANAI UN NOVĒRŠANAI

Riska Nr.	Pasākuma apraksts	Termiņš	Atbildīgā persona
1.			
2.			

II Risku pārvaldība

17. Rīcību ar riskiem nosaka pamatojoties uz drošības pasākumu izmaksu un iespējamo materiālo un nemateriālo zaudējumu sabalansētību:

17.1. akceptēt risku;

17.2. novērst vai mazināt risku (piemēram, ieviešot atbilstošas kontroles);

17.3. nodot risku trešajām pusēm (piemēram, izmantojot apdrošināšanas pakalpojumus).

18. Riskus, kuru novērtējums atbilst zemam līmenim, Risku pārvaldnieks neiekļauj IS drošības risku pārvaldības plānā.

19. Risku pārvaldnieks IS drošības risku pārvaldības plānā iekļauj augsta līmeņa riskus.

20. Riskiem, kuru novērtējums atbilst vidējam līmenim, veic padziļinātu to izvērtēšanu, apzinot to novēršanai vai ietekmes mazināšanai nepieciešamos veicamos pasākumus un to samērību attiecībā pret attiecīgo risku:

20.1. gadījumā, ja attiecīgā riska novēršanai vai ietekmes mazināšanai nepieciešamo veicamo pasākumu izmaksas ir lielākas nekā iespējamie zaudējumi, Iestādes vadība lemj par riska akceptēšanu;

20.2. gadījumā, ja attiecīgā riska novēršanai vai ietekmes mazināšanai nepieciešamo veicamo pasākumu resursu ietilpība ir mazāka nekā riska iestāšanās sekas, risku iekļauj IS drošības risku pārvaldības plānā.

21. Riskiem, kuru kopējais novērtējums atbilst augstam līmenim, kā arī vidējam līmenim, Risku pārvaldnieks sagatavo veicamo pasākumu aprakstus to novēršanai vai riska iestāšanās iespējamības vai atstāto seku līmeņa mazināšanai.
22. Pēc riska novēršanai vai mazināšanai veicamo pasākumu apraksta sagatavošanas, Risku pārvaldnieks nosaka veicamo pasākumu izpildes termiņus, nepieciešamos finanšu līdzekļus, laika un Iestādes nodarbināto resursus, kā arī potenciālo atbildīgo personu par veicamo pasākumu realizāciju.
23. Ja nepieciešami papildus resursi veicamo pasākumu realizācijai, piemēram, citas struktūrvienības nodarbināto resursi, Risku pārvaldnieks iesniedz IS drošības risku pārvaldības plānu apstiprināšanai Iestādes vadībai.
24. Ja noteiktu pasākumu veikšanai nepieciešamos finanšu vai cilvēku resursus nepiešķir vai piešķir nepietiekamā apmērā, Risku pārvaldnieks koriģē risku mazināšanas pasākumu aprakstu, nosakot veicamo pasākumu minimumu, kuru realizācija nodrošina identificētā riska iestāšanās varbūtības vai atstāto seku līmeņa samazināšanu bez papildus finanšu resursu piesaistes vai atbilstoši pieejamajiem finanšu vai cilvēku resursiem un Risku pārvaldnieks iesniedz IS drošības risku pārvaldības plānu apstiprināšanai Iestādes vadībai.

III Risku uzraudzība

25. Risku pārvaldnieks, atbilstoši IS drošības risku pārvaldības plānā definēto veicamo pasākumu izpildes termiņiem, veic pārbaudes par risku mazināšanas vai novēršanas pasākumu realizāciju, atzīmējot realizētos pasākumus.
26. Gadījumos, kad nepieciešamie pasākumi nav tikuši realizēti iepriekš noteiktajā termiņā, Risku pārvaldnieks kopā ar personu, kura ir atbildīga par attiecīgā pasākuma realizāciju, apzina apstākļus, kas ir kavējuši attiecīgo pasākumu realizēt sākotnēji paredzētajā termiņā un sagatavo priekšlikumus jauna pasākuma realizācijas termiņa noteikšanai, kā arī nepieciešamības gadījumā nosaka papildus veicamās darbības pasākuma ieviešanas nodrošināšanai.
27. Pēc identificētā riska novēršanas vai mazināšanas veicamā pasākuma izpildes, Risku pārvaldnieks veic atkārtotu riska novērtējumu.