

**IEKŠĒJIE NOTEIKUMI**

2023. gada 28. septembrīNr.8

**APSTIPRINĀTI**

ar Limbažu novada domes

28.09.2023. sēdes lēmumu Nr.718

(protokols Nr.11, 10.)

**LiMBažu novada PAŠVALDĪBAS**

**Informācijas sistēmu drošības politikA**

*Izdoti saskaņā ar*

*Informācijas tehnoloģiju drošības likuma 8. pantu un* *Ministru kabineta 28.07.2015. noteikumu Nr. 442 “Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām” 13. un 15.punktu*

# Vispārīgie noteikumi

1. Informācijas sistēmu drošības politikas mērķis ir noteikt kārtību, kādā tiek īstenota Limbažu novada pašvaldības domes izveidoto iestāžu, aģentūru un struktūrvienību (turpmāk – Pašvaldība) informācijas sistēmu (turpmāk – IS) un tehnisko resursu aizsardzība pret ārējiem un iekšējiem drošības apdraudējumiem, ievērojot ārējos normatīvajos aktos noteiktās prasības pieņemama IS drošības riska līmeņa noteikšanai, lai tiktu nodrošināta Pašvaldības IS nepārtraukta un kvalitatīva darbība.
2. IS drošības politikā lietoti šādi termini un saīsinājumi:
	1. **Informācijas tehnoloģijas (turpmāk – IT)** – tehnoloģijas, kuras tām paredzēto uzdevumu izpildei veic informācijas elektronisko apstrādi (t.sk. izveidošanu, dzēšanu, glabāšanu, attēlošanu vai pārsūtīšanu);
	2. **Informācijas resursi (turpmāk – IR)** – strukturēti dati, kas tiek izmantoti Pašvaldības darbībai nepieciešamās informācijas elektroniskās apstrādes procesā ar IT, un tiek glabāti datu bāzēs vai datņu veidā serveros, datoros, kā arī citos informācijas nesējos neatkarīgi no to veida;
	3. **Tehniskie resursi (turpmāk – TR)** – datori, serveri, datortīklu aparatūra un komunikāciju līnijas, kā arī visas pārējās IT iekārtas un nesējvide, kas nepieciešama informācijas apstrādei (tai skaitā aparātprogrammatūra, serveru un datoru operētājsistēmas, datu bāzu vadības sistēmas, lietojumprogrammas, mobilās lietotnes un jebkāda cita veida programmatūra);
	4. **Informācijas sistēma (turpmāk – IS)** – ir noteikts un savstarpēji saistīts IR un TR kopums, kas izveidots vai pielāgots, lai sniegtu nepieciešamo atbalstu Pašvaldības funkciju un citu uzdevumu izpildes nodrošināšanai;
	5. **IS pārzinis** — jebkāda veida institūcija, kas normatīvajos aktos noteiktajā kārtībā organizē un vada IS darbību, un tās īpašumā vai valdījumā atrodas IS nepieciešamie IR un TR;
	6. **IR turētājs** – Pašvaldības darbinieks, kas atbildīgs par vienu vai vairākiem darbības procesiem organizācijā, kā arī rīkojas ar to nodrošināšanai nepieciešamiem IR un nodrošina to uzturēšanu;
	7. **TR turētājs** – Pašvaldības darbinieks vai ārpakalpojuma sniedzējs, kas Pašvaldības uzdevumā rīkojas ar TR un nodrošina to uzturēšanu;
	8. **IR vai TR aizbildnis** – Pašvaldības darbinieks, kurš veic IR vai TR valdītāja pienākumus viņa pārziņā nodotajiem IR vai TR (tas skaitā to daļām);
	9. **IS drošība** – organizatorisko un tehnisko pasākumu kopums, ar kuru palīdzību tiek nodrošināta informācijas pieejamība, integritāte un konfidencialitāte Pašvaldībā;
	10. **IS drošības pārvaldnieks** – Pašvaldības vadības noteikts darbinieks vai ārējā IS drošības pārvaldības pakalpojuma sniedzēja pārstāvis, kurš Pašvaldībā īsteno IS drošības pārvaldību;
	11. **IS lietotājs** – jebkura persona, kurai tiek piešķirtas IS pieejas tiesības konkrētu uzdevumu izpildei vai informācijas piekļuvei;
	12. **Identitāte** – fiziskās personas datu un tai piemītošo fizisko īpašību vai valdījumā esošu rādītāju kopums, ar kuras palīdzību IS atšķir kādu fizisko personu no citas fiziskās personas;
	13. **Tehnoloģiskā identitāte** – rādītāju kopums, ar kuru palīdzību IS atšķir kādu IT procesu no cita IT procesa;
	14. **Auditācijas pieraksti** – analīzei pieejamais, IS ar jebkāda veida identitāti veikto darbību (piekļūšana, datu ievade, mainīšana, dzēšana, izvade) atspoguļojums;
	15. **Apdraudējums** – jebkurš ārējais vai iekšējais notikums, kas var nelabvēlīgi ietekmēt Pašvaldību vai tās IS un rezultātā radīt Pašvaldībai materiālos vai cita veida zaudējumus;
	16. **Datorvīruss** – programmatūras kods, kas spējīgs patstāvīgi iekļauties citas datorprogrammas kodā vai mainīt datus;
	17. **IT drošības nepilnība** – IT sistēmas vai elektronisko sakaru tīkla izveides, uzturēšanas vai pārveidošanas gaitā tīši vai nejauši radīta sistēmiska vājība, kuras rezultātā var tikt apdraudēta IS integritāte, pieejamība vai konfidencialitāte.
	18. **Ievainojamība** – nepilnība vai trūkums, kas ļauj, kādam noteiktam apdraudējumam īstenoties un ietekmēt IS, kā arī tās IR un TR drošību;
	19. **Drošības pārkāpums** – notikums, kurš izraisa informācijas vai pašas IS konfidencialitātes, integritātes vai pieejamības zaudējumu;
	20. **Drošības incidents** – jebkurš notikums, kurš var tikt konstatēts, veicot IT sistēmu lietošanu un uzraudzību, nav IT sistēmas vai servisa (pakalpojuma) standarta (tipveida) darbības sastāvdaļa un:
		1. kurš izraisa vai var izraisīt neplānotu dīkstāvi (pieejamības kritērijs);
		2. pasliktina sistēmas vai servisa (pakalpojuma) darbības kvalitāti un informācijas veselumu (integritātes kritērijs);
		3. apzinātas, tiešas vai netiešas darbības rezultātā rada vai var radīt konfidenciālas informācijas nesankcionētu noplūdi (konfidencialitātes kritērijs);
	21. **Risks** – identificēta ārējā vai iekšējā IS drošības apdraudējuma iestāšanās rezultātā Pašvaldībai nodarīto zaudējumu vai kaitējuma iespējamība un būtiskums;
	22. **Risku valdītājs** – IR vai TR turētājs, kura pārvaldīto resursu apdraud identificētais risks;
	23. **Risku analīze** – process, IS un IT drošības nepilnību un visus iespējamo apdraudējumu un to īstenošanās iespējamību un seku izvērtēšanai, lai piemērotu atbilstošus drošības līdzekļus identificēto risku samazināšanai un nodrošinātu drošības riska mazināšanas pasākumos izmantojamo līdzekļu samērojamību ar iespējamiem zaudējumiem vai radīto kaitējumu, kas Pašvaldībai, IS lietotājiem vai trešajām pusēm varētu rasties drošības incidenta dēļ;
	24. **Risku pārvaldīšana** – informācijas sistēmas risku identificēšana, novērtēšana, samazināšana un kontrolēšana, ar mērķi mazināt risku līdz Pašvaldībai pieņemamam līmenim.

# IS drošības politikas mērķi un pamatnostādnes

1. IS drošības politikas mērķis ir:
	1. drošības pārvaldības atbilstību normatīvajiem aktiem un standartiem;
	2. nodrošināt informācijas pieejamību;
	3. nodrošināt informācijas integritāti;
	4. nodrošināt informācijas konfidencialitāti;
	5. aizsargāt IS informācijas resursus;
	6. aizsargāt IS tehniskos resursus;
	7. noteikt IS drošības apdraudējumus;
	8. novērtēt IS drošības riskus;
	9. atklāt IS drošības incidentus;
	10. pašvaldības IS raksturojumu un analīzi;
	11. IS drošības politikas mērķus un pamatnostādnes;
	12. IS drošības pārvaldības organizācijas principus;
	13. atjaunot IS darbību pēc drošības incidentiem;
	14. IS drošības pārvaldību.
2. Pārzinis nodrošina, ka tā rīcībā esošā informācija tiek apstrādāta, glabāta un
pārvaldīta droši un pārbaudāmi, nosakot IS lietotājiem skaidras prasības
IS izmantošanā, kā arī organizē IS aizsardzību no ārējiem un iekšējiem, apzinātiem un nejaušiem apdraudējumiem.
3. IS lietotājus iepazīstina ar šiem noteikumiem pirms darba uzsākšanas institūcijās.
4. Par tehniskajiem resursiem atbildīgā persona kontrolē šo un citu pakārtoto noteikumu ievērošanu:
	1. Informācijas sistēmas lietošanas noteikumi;
	2. Informācijas sistēmu atjaunošanas plāns;
	3. Informācijas sistēmu drošības riska pārvaldības plāns;
	4. Informācijas sistēmu drošības iekšējie noteikumi.
5. IS drošības politiku izdod Pašvaldība un apstiprina Pašvaldības vadītājs.
6. IS drošības politika ir saistoša:
	1. visiem Pašvaldības darbiniekiem, ārpakalpojuma sniedzējiem un darbuzņēmējiem, kuri izmanto Pašvaldības pārziņā vai turējumā esošās IS, kā arī to informācijas un tehniskos resursus;
	2. visiem Pašvaldības darbiniekiem, ārpakalpojuma sniedzējiem un darbuzņēmējiem, kuri ir iesaistīti IS drošības pārvaldības aktivitātēs.
7. Pašvaldības IS drošības politiku un tai saistošos informācijas drošības jomā pieņemtos iekšējos normatīvos aktus IS drošības pārvaldnieks pārskata reizi gadā, kā arī gadījumos:
	1. ja plānotās vai veiktās izmaiņas IS var ietekmēt tās drošību;
	2. ja ir mainījušies vai ir atklāti jauni IT drošības apdraudējumi;
	3. ja pēkšņi pieaug drošības incidentu skaits vai ir noticis būtisks drošības incidents;
	4. ja plānotās izmaiņas Pašvaldības organizatoriskajā struktūrā skar IT drošības pārvaldības procesa organizāciju;
	5. ja izdarīti grozījumi ārējos normatīvajos aktos, kas regulē IS darbību vai IT drošības pārvaldības procesa nodrošināšanu Pašvaldībā.

# **IS drošības atbilstība prasībām**

1. Pašvaldības IS drošības pārvaldību organizē ievērojot šādu normatīvo aktu prasības:
	1. Informācijas tehnoloģiju drošības likums (turpmāk – IT drošības likums);
	2. Fizisko personu datu apstrādes likums;
	3. Eiropas Parlamenta un Padomes Regula (ES) 2016/679 (2016. gada 27. aprīlis) par fizisku personu aizsardzību attiecībā uz personas datu apstrādi un šādu datu brīvu apriti un ar ko atceļ Direktīvu 95/46/EK (turpmāk – VDAR);
	4. Ministru kabineta 2015. gada 28. jūlija noteikumi Nr. 442 "Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām" (turpmāk – MK noteikumi Nr.442);
	5. Valsts informācijas sistēmu likums.
2. Pašvaldība IS drošības pārvaldību organizē ņemot vērā Interneta drošības centra (CIS) izstrādātos kontroles mehānismus, kā arī izmanto citas iekšējās metodoloģijas, informācijas drošības labās prakses un principus.
3. Pārzinis organizē IS drošības dokumentācijas atbilstības normatīvo aktu prasībām pārskatīšanu. Ja tiek konstatēti būtiski trūkumi, Pārzinis veic pasākumus to novēršanai.
4. Izmaiņas veicamas arī šādos gadījumos:
	1. mainījušies vai ir atklāti jauni IS drošības apdraudējumi;
	2. pieaug IS drošības incidentu skaits vai ir noticis nozīmīgs drošības incidents;
	3. izmaiņas Pārziņa organizatoriskajā struktūrā skar IS drošības vadības organizāciju;
	4. izdarīti grozījumi normatīvajos aktos, kas regulē IS darbību.
5. Pašvaldības IS drošības pārvaldības dokumentācijas kopu veido:
	1. Pašvaldībai saistoši IS drošības noteikumi (t.sk. drošības tiesiskās, organizatoriskās, loģiskās un fiziskās aizsardzības, kā arī informācijas aprites, apstrādes, izmaiņu un uzglabāšanas drošības kārtības un prasības);
	2. Pašvaldības normatīvie akti, kas nosaka detalizēti izvērstu informācijas drošības pārvaldības procesu kārtību (t.sk. IS resursu klasifikācijas kārtību, lietotāju tiesību pārvaldības kārtību, risku pārvaldības kārtību, risku novēršanas metodoloģiju);
	3. Pašvaldības iekšējie noteikumi, kas nosaka Pašvaldības pārziņā vai turējumā esošas IS drošības noteikumus;
	4. Pašvaldības pārziņā vai turējumā esošu IS resursu drošības pārvaldības procedūras un instrukcijas;
	5. IS resursu drošības risku pārvaldības plāni, kas tiek izstrādāti paaugstinātas drošības IS;
	6. IS resursu darbības atjaunošanas plāni, kas tiek izstrādāti paaugstinātas drošības IS.

# Pašvaldības IS apraksts un drošības risku līmeņi

1. Pašvaldības iestādes un aģentūras ir IS pārziņi tām IS, kuras tās ir izveidojušas vai ieviesušas savām tiešajām vajadzībām.
2. Pašvaldības IS TR ir izvietoti Pašvaldības darba telpās vai datu centros. Pašvaldība IS TR tehnisko apkopi un administrēšanu var nodot ārpakalpojumu sniedzējiem.
3. Pašvaldības darbinieku, kuri veic IS uzturēšanu un uzraudzību, pienākumi, atbildība un savstarpējā aizvietojamība noteikta katra darbinieka amata aprakstā.
4. Pašvaldībai jānodrošina, ka risku ierobežošanas un darbības nepārtrauktības nodrošināšanas izmaksas ir samērojamas ar iespējamajiem zaudējumiem, kas varētu rasties šo risku īstenošanās vai Pašvaldības IS darbības pārtraukšanas gadījumos.
5. Pašvaldības IS iedala divās kategorijās – pamata un paaugstinātas drošības sistēmas. Savukārt tās IS, kurām nav noteikta pieejamības, integritātes vai konfidencialitātes klase, tiek uzskatītas par neklasificētām.
6. Pašvaldības IS un attiecīgo IR un TR turētāju sarakstu, kā arī IS klasifikāciju atbilstoši MK noteikumu NR.442 prasībām[[1]](#footnote-1) sagatavo atbilstoši 1. pielikuma paraugam un to apstiprina Pašvaldības vadītājs vai tā pilnvarota persona.
7. Pašvaldības klasificēto IS drošības pasākumi tiek plānoti, balstoties uz IS drošības politikā noteiktajām vadlīnijām un riska analīzes laikā izstrādātajiem novērtējumiem, tā, lai IS drošības pasākumi tiktu realizēti ar optimāliem resursiem.
8. Pašvaldība veic IS risku analīzi saskaņā ar iekšējos noteikumos par IS drošības riska pārvaldības plānu noteikto metodoloģiju.
9. Pašvaldības paaugstinātas drošības IS risku analīze tiek veikta vismaz reizi gadā, kā arī šādos gadījumos, ja:
	1. plānotās izmaiņas var ietekmēt IS drošību;
	2. mainījušies vai ir atklāti jauni drošības apdraudējumi IS;
	3. pēkšņi pieaug IS drošības incidentu skaits vai ir noticis būtisks drošības incidents;
	4. izmaiņas institūcijas organizatoriskajā struktūrā skar IS drošības vadības organizāciju;
	5. izdarīti grozījumi normatīvajos aktos, kas regulē IS darbību.
10. Pašvaldības pamata drošības IS risku analīze tiek veikta to sākotnēji pieņemot ekspluatācijā vai arī pēc IR turētāja pieprasījuma, ja:
	1. plānotās izmaiņas viennozīmīgi ietekmēs IS drošību;
	2. ir atklāti tādi drošības apdraudējumi IS, kurus IT drošības nepilnību novēršanas procesā patlaban nav iespējams novērst;
	3. noticis Būtisks drošības incidents, kam par iemeslu kalpojusi tāda IT drošības nepilnība, kuru pēc Drošības incidenta seku novēršanas nebūs iespējams novērst;
	4. izmaiņas institūcijas organizatoriskajā struktūrā būtiski skar IS drošības vadības organizāciju;
	5. izdarīti būtiski grozījumi normatīvajos aktos, kas regulē IS darbību.
11. Plānojot jaunu IS izstrādi vai iegādi, IR turētājs informē IS drošības pārvaldnieku par IS iepirkuma līguma dokumentācijā plānotajām biznesa un drošības prasībām, lai kopīgi identificētu iespējamos riskus un izvērtētu nepieciešamību veikt jaunās IS sākotnējo Risku analīzi, ievērojot Pašvaldībā noteikto kārtību.
12. Pašvaldības IS var izstrādāt ārpakalpojumu sniedzēji, kuri atsevišķos gadījumos veic arī to uzturēšanu vai TR izmitināšanu. Līgumu izpildes uzraudzību nodrošina konkrēto IR turētāji.
13. IS izstrādi, iegādi, ieviešanu un papildināšanu pārrauga IR turētājs, saskaņojot plānojamās un veicamās aktivitātes ar TR turētāju.
14. Pirms IS ieviešanas tiek veikta tās pieņemšanas testēšana, ko veic IR turētājs vai tā atsevišķi norīkoti IS lietotāji. Tikai pēc pozitīviem lietotāju testēšanas rezultātiem atbilstošā IS vai izmaiņas tajā var tikt uzstādītas uz Pašvaldības TR.
15. Veicot IS izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu sistēmās glabāto datu integritātei, tādēļ šādiem nolūkiem tiek izmantota IS sistēmas testa vide, kas tiek izvietota uz Pašvaldības TR, vai nodrošinot piekļuves tiesības attiecīgajiem IS lietotājiem, gadījumā, ja IS testa vide atrodas pie IS izstrādātāja.
16. TR turētājs ne retāk kā 1 (vienu) reizi 2 (divos) gados nodrošina IS darbības atjaunošanas procesos iesaistītā personāla apmācību.
17. TR turētājs ir atbildīgs par IS darbības atjaunošanas plāna izpildi, kā arī tajā paredzēto pasākumu izpildes regulāru kontroli.
18. Pašvaldības IS nepārtrauktas darbības laiks ir darba dienās – pirmdienās no 8:00 līdz 18:00. no otrdienas līdz ceturtdienai plkst. 8.00 līdz 17.00, piektdienās no 8:00 līdz 16:00, pirmssvētku dienās darba laiks tiek saīsināts par 1 stundu.
19. Pašvaldības IS darbības atjaunošanu avārijas gadījumā veic tā, lai atjaunošanai nepieciešamais laiks nepārsniegtu 1 (vienu) darba dienu vai citu IR valdītāja noteiktu laika periodu.
20. Pašvaldības IS tiek nodrošināta informācijas uzkrāšana auditācijas pierakstos, ja vien IR vai TR nepastāv darbības žurnālu datņu veidošanas iespēja, lai nodrošinātu auditācijas pierakstu saglabāšanu saskaņā ar MK noteikumos Nr.442 noteikto[[2]](#footnote-2). Pašvaldības IT atbalsta darbinieki nodrošina šīs informācijas regulāru pārskatīšanu ikdienā, kā arī IS avāriju, darbības problēmu un drošības pārkāpumu gadījumā, pēc nepieciešamības piesaistot IS drošības pārvaldnieku.

# IS drošības pārvaldības galvenie principi

1. Par Pašvaldības IS drošību atbildīgie darbinieki, ārpakalpojumu sniedzēji un darbuzņēmēji īsteno operacionālās drošības plānotās un pēc faktiskās situācijas nepieciešamās aktivitātes, saskaņā ar IS drošības politikas sadaļā II. IS drošības atbilstība prasībām noteikto ietvaru.
2. Pašvaldības izpilddirektors:
	1. atbild par IS drošības nodrošināšanu;
	2. nosaka par IS drošības pārvaldību atbildīgo personu;
	3. nodrošina nepieciešamos līdzekļus un atbalstu IS drošības politikas ieviešanai, uzturēšanai un pilnveidošanai;
	4. nosaka pienākumu un atbildības sadalījumu attiecībā uz IS drošību;
	5. apstiprina visu pārējo Pašvaldībai nepieciešamo IS drošības pārvaldības dokumentāciju, saskaņā ar 14.punktā noteikto, izņemot IS drošības politiku.
3. Par IS drošības pārvaldību atbildīgā persona ir ar Pašvaldības vadītāja rīkojumu iecelts IS drošības pārvaldnieks, kurš:
	1. organizē ar IS drošības pārvaldību saistīto aktivitāšu īstenošanu Pašvaldībā, saskaņā ar 2. punktā norādīto normatīvo aktu prasībām;
	2. organizē IS risku analīzi un koordinē visu nepieciešamo aktivitāšu veikšanu risku pārvaldīšanai;
	3. veic nepieciešamās IS drošības dokumentācijas izstrādi un uzturēšanu;
	4. veic noteikto drošības prasību ievērošanas uzraudzību, organizē IS drošības pārbaudes un konstatēto IT drošības nepilnību un ievainojamību novēršanu;
	5. veic drošības incidentu izmeklēšanu un organizē nepieciešamos pasākumus, lai novērstu drošības incidenta radītās sekas un nepieļautu šāda veida incidenta atkārtošanos turpmāk;
	6. nodrošina darbinieku apmācību IS drošības jomā;
	7. informē IT drošības incidentu novēršanas institūciju CERT.LV būtiska drošības incidenta gadījumā un nekavējoties organizē visas nepieciešamās darbības tā novēršanai, kā arī vienojas ar IT drošības incidentu novēršanas institūciju par nepieciešamā atbalsta saņemšanu.
4. Pašvaldības IS drošības pārvaldībā ir noteiktas četru personu atbildības grupas:
	1. IS lietotājs;
	2. IR turētājs;
	3. TR turētājs;
	4. IR vai TR aizbildnis.
5. IS lietotājs:
	1. iepazīstas un apņemas ievērot informācijas drošības jomā pieņemto iekšējo normatīvo aktu un personu datu aizsardzības prasības;
	2. nekavējoties ziņo Pašvaldības IT nodaļai par IS identificētajiem riskiem, informācijas drošības notikumiem un incidentiem;
	3. pēc nepieciešamības informē IR turētāju par iespējamajiem vai konstatētajiem IT drošības pārkāpumiem un nepilnībām IT drošībai;
	4. ne retāk kā reizi gadā iziet darbinieku instruktāžu IT drošības jautājumos.
6. IR turētājs:
	1. atbild par IS piesaistīto IR lietojumu un saturu;
	2. nosaka IR ilgtermiņa uzglabāšanas kārtību;
	3. klasificē savā atbildībā esošos IR un nosaka tiem nepieciešamās drošības prasības;
	4. nosaka nepieciešamās darbības IR drošības nepilnību novēršanai pārvaldībā esošām IS;
	5. sadarbībā ar TR turētāju, IS drošības pārvaldnieka vadībā un pārraudzībā piedalās risku analīzes veikšanā, pieņem vai nodod atkārtotai analīzei risku analīzes ziņojumu un IS drošības riska pārvaldības plānu, seko apstiprinātajā plānā ietverto rīcību izpildei;
	6. nosaka piekļuves kārtību IS piesaistītajiem IR;
	7. apstiprina IS lietotāju piekļuves tiesības;
	8. nodrošina lietotāju uzskaiti un apmācību darbam ar IS;
	9. nosaka prasības IR atjaunošanai un sadarbojas ar TR valdītājiem (tai skaitā aizbildņiem) IS funkcionalitātes un drošības jautājumos.
7. TR turētājs:
	1. atbild par IS tehnisko resursu iegādi, izstrādi, darbību un uzturēšanu;
	2. patstāvīgi seko līdzi aktuālai informācijai par aparatūras un programmatūras jauninājumiem, lai laikus novērstu zināmās IT drošības ievainojamības un trūkumus TR;
	3. ievieš un nodrošina IS tehniskos un loģiskos aizsardzības pasākumus, saskaņā ar Pašvaldības iekšējo normatīvo aktu prasībām, ievērojot IR noteiktās prasības un IS drošības pārvaldnieka sniegtos norādījumus;
	4. atbild par IS pieejas tiesību pārvaldību, sadarbībā ar IR un aizbildņiem;
	5. atbild par IS atjaunošanas plāna izstrādi un regulāro darbības pārbaudi, kā arī veic IS darbības atjaunošanas pasākumus, ja IS darbība ir traucēta vai neiespējama;
	6. piedalās risku analīzē, nosaka ar TR saistītus IS apdraudējumus un novērtē šo apdraudējumu īstenošanās varbūtību;
	7. informē IS drošības pārvaldnieku par tādiem drošības notikumiem, kas varētu tikt klasificēti kā drošības incidenti;
	8. sadarbībā ar IS drošības pārvaldnieku īsteno IS drošības pārbaudi un IT drošības nepilnību novēršanu;
	9. reģistrē un apkopo informāciju par IS kļūdām, IS lietotāju jautājumiem un citām problēmām;
	10. sadarbojas ar IR turētājiem (tai skaitā aizbildņiem) IS funkcionalitātes un drošības jautājumos;
	11. nodrošina TR drošības prasību iekļaušanu ārpakalpojumu līgumos, ja TR izmitināšanu nodrošina ārpakalpojumu sniedzēji.
8. Katras IS IR un TR turētājs tiek noteikts ar Pašvaldības vadītāja vai tā pilnvarotas personas rīkojumu.
9. Pēc IR vai TR turētāja ieteikuma Pašvaldības vadītājs vai tā pilnvarota persona var nozīmēt IR un TR aizbildņus, kuri pilda IR un TR turētāja pienākumus attiecībā uz viņa pārziņā nodotajiem IR, TR vai to daļu. IR vai TR turētājs attiecīgi koordinē un pārvalda IR vai TR aizbildņu darbu uzticētajā jomā.
10. Pašvaldības darbinieku, kuri veic IS uzturēšanu un uzraudzību, pienākumi, atbildība un savstarpējā aizvietojamība tiek noteikta katra Darbinieka amata aprakstā.
11. Par Pašvaldības IS drošības pārvaldības funkcijas uzraudzību atbild Pašvaldības vadītājs, savukārt par tās ikdienas darbu ietvaros veicamo drošības aktivitāšu izpildes kontroli ir atbildīgi iesaistīto Pašvaldības darbinieku tiešie vadītāji, attiecīgā TR turētājs un IS drošības pārvaldnieks.

# IS drošības pārvaldības organizācija

1. Struktūrvienību, iestāžu un aģentūru vadītāji ir atbildīgi par viņu pakļautībā vai uzraudzībā esošajiem IS lietotājiem, kā arī nodrošina, ka personāls apzinās IS drošības politikas esamību, lai pildītu savus darba pienākumus, ievērojot tajā noteikto regulējumu.
2. Iepazīšanos ar IS drošības politiku un apņemšanos ievērot tās prasības Pašvaldības darbinieks apliecina, parakstot Apliecinājumu par IS drošības politikas ievērošanu (turpmāk – apliecinājums) (2. pielikums).
3. Darbinieku iepazīstināšanu ar IS drošības politiku un apliecinājuma pieņemšanu veic Pašvaldības Administratīvā nodaļas personāla speciālisti vai Pašvaldības iestādes vadītājs un Apliecinājums glabājas attiecīgā darbinieka personas lietā.
4. Atbildīgais par Pašvaldības ārpakalpojuma sniedzēju un darbuzņēmēju iepazīstināšanu ar IS drošības politiku un jebkādu citu tai saistošo dokumentāciju ir atbilstošās vienošanās vai līguma koordinators.
5. Ikviena Pašvaldības darbinieka, ārpakalpojuma sniedzēja un darbuzņēmēja pienākums ir ievērot arī jebkādus citus Pašvaldības rīkojumus un saistošos normatīvos aktus IS drošības pārvaldības jomā. Par Pašvaldības darbinieku iepazīstināšanu ar jebkādiem citiem IS drošības politikai saistošajiem dokumentiem ir atbildīgi šo darbinieku tiešie vadītāji.
6. Pašvaldības darbinieki, ārpakalpojuma sniedzēji un darbuzņēmēji ir atbildīgi par IS drošības prasību ievērošanu un IS lietošanu, saskaņā ar Pašvaldībā noteikto kārtību, kā arī visām darbībām, kuras tiek veiktas ar to IS lietotāja vārdu.
7. Pašvaldības darbinieka pienākums ir nekavējoties ziņot savam tiešajam vadītājam vai Pašvaldības IT atbalsta dienestam par iespējamajiem un konstatētajiem drošības notikumiem vai incidentiem, ievērojot Pašvaldībā noteikto kārtību.
8. Jebkurš IS lietotājs ir tiesīgs attiecīgā IR turētājam pieprasīt skaidrojumu par IS drošības jautājumiem, kā arī iesniegt priekšlikumus IS drošības uzlabošanai un saņemt nepieciešamo kompetences atbalstu no IS drošības pārvaldnieka.
9. Lai izglītotu Pašvaldības darbiniekus par IS Drošības politikā noteikto regulējumu, aktuālajiem informācijas drošības apdraudējumiem un paaugstinātu izpratni drošības riska jautājumos, Pašvaldība vismaz reizi gadā nodrošina tās darbiniekiem apmācības IS drošības jautājumos.
10. IS drošības pārvaldnieks reizi gadā veic Pašvaldības IS drošības pārvaldības snieguma novērtējumu un sagatavo IS drošības pārvaldības ikgadējo pārskatu, kas tiek iesniegts Pašvaldības vadībai vai tās pilnvarotam pārstāvim.
11. Pašvaldība organizē IS drošības auditus, ievērojot gan MK noteikumos Nr.442 noteikto[[3]](#footnote-3), gan ņemot vērā iekšējo regulējumu IS drošības jomā. Paaugstinātas drošības IS auditos konstatētie būtiskie riski tiek iekļauti attiecīgās Pašvaldības IS drošības riska pārvaldības plānā.
12. Ja Pašvaldība nepiesaista ārpakalpojumu sniedzēju IS drošības pārbaudes veikšanai, tad IS drošības pārvaldnieks reizi gadā organizē klasificēto IS drošības pārbaudi, pārbaudot, vai:
	1. IS un tās IT netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;
	2. IS ir atspējoti tie lietotāji, kuriem IR nav apstiprinājis vai ir anulējis pieejas tiesības;
	3. IS ir uzstādīti pieejamie programmatūras atjauninājumi, iepriekš izvērtējot to uzstādīšanas iespējamību no TR puses;
	4. IS darbības nodrošināšanai netiek izmantotas tādas IT, kas satur publiski zināmas nenovērstas drošības ievainojamības, vai arī tādas IT, kam beidzies ražotāja tehniskais atbalsts un to turpmāka izmantošana rada riskus IS drošībai.
13. IS drošības pārbaudes var tikt īstenotas arī izmantojot specializēto programmatūru, kuras izstrādātājs vai ražotājs ir juridiska persona, kas reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, vai fiziska persona, kas ir Latvijas Republikas valstspiederīgais, NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas valsts pilsonis.
14. IS drošības pārbaude Pašvaldība var tikt ierosināta arī atsevišķai IS – pēc IR turētāja pieprasījuma, pirms IS nodošanas ekspluatācijā vai publiskas pieejamības nodrošināšanas.

# **Noslēguma jautājumi**

1. Šos noteikumus pārskata vismaz reizi gadā, kā arī:
	1. ja izmaiņas IS var ietekmēt IS drošību;
	2. ja mainījušies vai atklāti jauni IS drošības apdraudējumi;
	3. ja pieaug IS drošības incidentu skaits vai noticis nozīmīgs incidents.

Limbažu novada pašvaldības

Domes priekšsēdētājs D. Straubergs

ŠIS DOKUMENTS IR PARAKSTĪTS AR DROŠU ELEKTRONISKO PARAKSTU UN SATUR LAIKA ZĪMOGU

**1. PIELIKUMS**

Limbažu novada pašvaldības

2023. gada 28. septembra iekšējiem noteikumiem Nr.8

“Limbažu novada pašvaldības informācijas sistēmu drošības politika”

INFORMĀCIJAS RESURSU REĢISTRS

|  |  |  |  |
| --- | --- | --- | --- |
| **Pieejamība** | **A**(neplānots IS nodrošinātā pakalpojuma pārtraukums ne lielāks par 4 h/mēnesī) | **B**(neplānots IS nodrošinātā pakalpojuma pārtraukums ne lielāks par 24 h/mēnesī) | **C**(neplānots IS nodrošinātā pakalpojuma pārtraukums lielāks par 24 h/mēnesī) |
| **Integritāte** | **A**(rada risku Pašvaldības pamatfunkciju nodrošināšanai un Latvijas Republikas nacionālajām interesēm) | **B**(rada risku Pašvaldības pamatfunkciju nodrošināšanai) | **C**(nerada risku Pašvaldības pamatfunkciju nodrošināšanai) |
| **Konfidencialitāte** | **A**(īpašo kategoriju personas dati, vai jebkāda cita informācija, kuras neatļauta izpaušana rada smagākas sekas nekā kaitējums Pašvaldības reputācijai) | **B**(ierobežotas pieejamības informācija, kuras neatļauta izpaušana rada kaitējumu Pašvaldības reputācijai) | **C**(publiski pieejama informācija, kuras neatļauta izpaušana nerada riskus Pašvaldībai) |
| **Prioritāte** | **1 (augsta)**IS darbības problēmas vai atteice rada augstu risku Pašvaldības funkciju nodrošināšanai - Pašvaldība nevar turpināt savu darbību, nav zināms risinājums | **2 (vidēja)**IS darbības problēmas vai atteice rada vidēju risku Pašvaldība funkciju nodrošināšanai - Pašvaldības darbība ir traucēta, ir iespējams risinājums | **3 (zema)**IS darbības problēmas vai atteice rada zemu risku Pašvaldības funkciju nodrošināšanai - Pašvaldības darbība ir apgrūtināta, ir zināms risinājums |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Nr. p.k.** | **IS raksturojums** | **Informācijas resursu turētājs (iestāde, struktūra, amats)** | **Tehnisko resursu turētājs (iestāde, struktūra, amats)** | **Informācijas sistēmas klasifikācija** |
| Pieejamības klase | Datu integritātes klase | Datu konfidencialitātes klase | Drošības līmenis | Prioritāte |
|  |  |  |  |  |  |  |  |  |

**2. PIELIKUMS**

Limbažu novada pašvaldības

2023. gada 28. septembra iekšējiem noteikumiem Nr.8

“Limbažu novada pašvaldības informācijas sistēmu drošības politika”

**Apliecinājums**

**par Informācijas sistēmu drošības politikas prasību ievērošanu**

Ar šo es, zemāk parakstījies, apliecinu:

1. Esmu iepazinies (-usies), izprotu un apņemos ievērot IS drošības politikā noteikto nosacījumu un prasību ievērošanu, kā arī apņemos ievērot drošības prasības, kas izriet no jebkādiem IS drošības politikai saistošajiem dokumentiem.
2. Apņemos neizmantot informāciju, kas saņemta no Limbažu novada pašvaldības, savu vai trešo personu interesēs, kā arī apņemos ievērot Fizisko personu datu apstrādes likuma un Informācijas atklātības likuma prasības.
3. Es piekrītu, ka, pārtraucot darba (līguma) attiecības ar Limbažu novada pašvaldību jebkādu iemeslu dēļ, es nekavējoties nodošu manā rīcībā nodoto programmatūru un tehnisko aprīkojumu, kā arī manā rīcībā esošos informācijas oriģinālus un kopijas, ko esmu saņēmis (usi) darba (līguma izpildes) laikā un kas ir manā rīcībā vai kas ir citādi tieši vai netieši manā pārvaldībā.
4. Apņemos saglabāt informācijas konfidencialitāti arī pēc darba (līguma izpildes) tiesisko attiecību izbeigšanas.

|  |  |  |  |
| --- | --- | --- | --- |
| \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Struktūrvienība un amats | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_/Paraksts/ | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Paraksta atšifrējums | \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_Datums |

1. 7. Lai valsts un pašvaldību institūciju sistēmu, kas nav kritiskās infrastruktūras informācijas sistēma vai sistēma, ko izmanto pamatpakalpojuma un digitālā pakalpojuma sniegšanai, iedalītu pamata vai paaugstinātas drošības sistēmā, par informācijas tehnoloģiju drošības pārvaldību atbildīgā persona (turpmāk – atbildīgā persona) to izvērtē atbilstoši šādai metodikai:

7.1. izvērtē šo noteikumu 13.5. apakšpunktā minēto risku pieņemamo līmeni un piešķir atbilstošo drošības (pieejamības, integritātes un konfidencialitātes) klasi:

7.1.1. ja sistēmas nodrošinātā pakalpojuma neplānots pārtraukums sistēmas paredzētajā darba laikā drīkst būt ilgāks par 24 stundām mēnesī (summāri), sistēmai piešķir C pieejamības klasi;

7.1.2. ja 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, sistēmai piešķir B pieejamības klasi;

7.1.3. ja sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par četrām stundām mēnesī (summāri), sistēmai piešķir A pieejamības klasi;

7.1.4. ja sistēmā glabāto datu integritātes apdraudējums nerada risku valsts un pašvaldību institūcijas pamatfunkciju nodrošināšanai, sistēmai piešķir C integritātes klasi;

7.1.5. ja atsevišķu sistēmā glabāto datu integritātes apdraudējums rada risku valsts un pašvaldību institūcijas pamatfunkciju nodrošināšanai, sistēmai piešķir B integritātes klasi;

7.1.6. ja sistēmā glabāto datu integritātes apdraudējums rada risku valsts un pašvaldību institūcijas pamatfunkciju nodrošināšanai vai atsevišķu sistēmā glabāto datu integritātes apdraudējums var apdraudēt Latvijas Republikas nacionālās intereses un pamatvērtības vai izraisīt katastrofu, sistēmai piešķir A integritātes klasi;

7.1.7. ja sistēma satur tikai publiski pieejamu informāciju vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde nerada risku valsts un pašvaldību institūcijai, sistēmai piešķir C konfidencialitātes klasi;

7.1.8. ja sistēmā tiek apstrādāta ierobežotas pieejamības informācija, izņemot sensitīvus personas datus, vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūdes vienīgās sekas ir iespējamais kaitējums valsts un pašvaldību institūcijas, citu institūciju vai Latvijas Republikas reputācijai, sistēmai piešķir B konfidencialitātes klasi;

7.1.9. ja sistēmā tiek apstrādāti sensitīvi personas dati vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde var radīt smagākas sekas nekā kaitējums valsts un pašvaldību institūcijas, citu institūciju vai Latvijas Republikas reputācijai, sistēmai piešķir A konfidencialitātes klasi;

7.2. ja sistēmai piešķirtas trīs B drošības klases vai vismaz viena A drošības klase, sistēma ir uzskatāma par paaugstinātas drošības sistēmu;

7.3. pārējos gadījumos sistēma ir uzskatāma par pamata drošības sistēmu. [↑](#footnote-ref-1)
2. Pamata drošības IS vismaz sešus mēnešus pēc ieraksta izdarīšanas, savukārt paaugstinātas drošības IS vismaz 18.mēnešu ilgā laika periodā. [↑](#footnote-ref-2)
3. Paaugstinātas drošības IS vismaz reizi divos gados pasūtot ārēju drošības dokumentācijas auditu un ielaušanās testu veikšanu. [↑](#footnote-ref-3)