*Projekts*

2015. gada Noteikumi Nr.

Rīgā (prot. Nr. .§)

**Kārtība, kādā valsts un pašvaldību institūcijas nodrošina informācijas un komunikācijas tehnoloģiju sistēmu, tajā skaitā valsts informācijas sistēmu, atbilstību minimālajām drošības prasībām**

Izdoti saskaņā ar Informācijas tehnoloģiju drošības likuma 8. panta piekto daļu un Valsts informācijas sistēmu likuma 4. panta otro daļu

**I. Vispārīgie jautājumi**

1. Noteikumi nosaka:
	1. valsts un pašvaldību institūciju (turpmāk – institūcijas) informācijas un komunikācijas tehnoloģiju minimālās drošības prasības un kārtību, kādā tiek nodrošināta valsts un pašvaldību informācijas un komunikācijas tehnoloģiju sistēmu (t.i., informācijas un komunikācijas tehnoloģiju sistēmu, kas ir valsts un pašvaldību institūciju pārziņā vai turējumā) atbilstība šīm prasībām;
	2. valsts informācijas sistēmu vispārējās drošības prasības.
2. Noteikumi neattiecas uz informācijas un komunikācijas tehnoloģiju sistēmām, kurās tiek veikta valsts noslēpuma, Ziemeļatlantijas līguma organizācijas (turpmāk – NATO), Eiropas Savienības un ārvalstu institūciju klasificētās informācijas vai informācijas dienesta vajadzībām apstrāde vai uzglabāšana, un uz kritiskās infrastruktūras informācijas sistēmām.
3. Noteikumi attiecas uz informācijas un komunikācijas tehnoloģiju sistēmām, tajā skaitā valsts informācijas sistēmām (turpmāk – sistēmas), kas ir testēšanas stadijā, kā arī sistēmām, kas nodotas lietošanā. Pārējās sistēmas stadijās (plānošanas, projektēšanas, izstrādes stadijas) jānodrošina atbilstoša informācijas, ko satur sistēma, aizsardzība.
4. Šajos noteikumos minētos par informācijas tehnoloģiju drošības pārvaldību atbildīgās personas pienākumus attiecībā uz valsts informācijas sistēmu veic sistēmas drošības pārvaldnieks.
5. Sistēmas drošību nodrošina pasākumu kopums, kurus īsteno, lai:
	1. nodrošinātu informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);
	2. nodrošinātu informācijas integritāti (pilnīgas un nemainītas informācijas saglabāšanu);
	3. nodrošinātu informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);
	4. aizsargātu sistēmas informācijas resursus (datnes (arī tās, kuras satur sistēmā glabājamo, apstrādājamo un sistēmas lietotājiem pieejamo informāciju) un sistēmas dokumentāciju);
	5. aizsargātu sistēmas tehniskos resursus (datorus, programmatūru, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību);
	6. noteiktu sistēmas drošības apdraudējumu (ar nodomu (tīši) vai aiz neuzmanības izdarītu darbību vai notikumu, kas var izraisīt sistēmas informācijas vai tehnisko resursu izmaiņas, bojājumu, iznīcināšanu vai nonākšanu tādu personu rīcībā, kuras nav tam pilnvarotas, vai kura dēļ piekļūšana sistēmas informācijas resursiem var būt traucēta vai neiespējama);
	7. novērtētu sistēmas drošības risku;
	8. atklātu sistēmas drošības incidentu;
	9. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.
6. Sistēmas dalāmas divās kategorijās – pamata un paaugstinātas drošības sistēmas.
7. Lai noteiktu katras sistēmas iedalījumu pamata vai paaugstinātas drošības sistēmā, par informācijas tehnoloģiju drošības pārvaldību atbildīgā persona (turpmāk – atbildīgā persona) to izvērtē atbilstoši šādai metodikai:
	1. izvērtē šo noteikumu 13.5. apakšpunktā minēto risku pieņemamo līmeni un piešķir attiecīgas drošības (t.i., pieejamības, integritātes un konfidencialitātes) klases:
		1. ja sistēmas nodrošinātā pakalpojuma neplānots pārtraukums sistēmas paredzētajā darba laikā drīkst būt ilgāks par 24 stundām mēnesī (summāri), tad sistēmai piešķir C pieejamības klasi,
		2. ja sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par 24 stundām (summāri) mēnesī, bet tas pieļaujams lielāks par 4 stundām (summāri) mēnesī, tad sistēmai piešķir B pieejamības klasi,
		3. ja sistēmas nodrošinātā pakalpojuma neplānotam pārtraukumam sistēmas paredzētajā darba laikā jābūt ne lielākam par 4 stundām mēnesī (summāri), tad sistēmai piešķir A pieejamības klasi,
		4. ja sistēmā glabāto datu integritātes apdraudējums nerada risku institūcijas pamatfunkciju nodrošināšanai, tad sistēmai piešķir C integritātes klasi,
		5. ja atsevišķu sistēmā glabāto datu integritātes apdraudējums rada risku institūcijas pamatfunkciju nodrošināšanai, tad sistēmai piešķir B integritātes klasi,
		6. ja sistēmā glabāto datu integritātes apdraudējums rada risku institūcijas pamatfunkciju nodrošināšanai vai atsevišķu sistēmā glabāto datu integritātes apdraudējums var apdraudēt Latvijas Republikas nacionālās intereses un pamatvērtības vai izraisīt katastrofu, tad sistēmai piešķir A integritātes klasi,
		7. ja sistēma satur tikai publiski pieejamu informāciju vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde nerada risku institūcijai, tad sistēmai piešķir C konfidencialitātes klasi,
		8. ja sistēmā tiek apstrādāta ierobežotas pieejamības informācija, izņemot sensitīvus personas datus, vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūdes vienīgās sekas ir iespējams kaitējums institūcijas, citu institūciju vai Latvijas Republikas reputācijai, tad sistēmai piešķir B konfidencialitātes klasi,
		9. ja sistēmā tiek apstrādāti sensitīvi personas dati vai sistēmā glabātās informācijas neatļauta izpaušana vai noplūde var novest pie smagākām sekām kā kaitējums institūcijas, citu institūciju vai Latvijas Republikas reputācijai, tad sistēmai piešķir A konfidencialitātes klasi.
	2. Ja sistēmai piešķirtas trīs B drošības klases vai vismaz viena A drošības klase, tad sistēma ir uzskatāma par paaugstinātas drošības sistēmu.
	3. Pārējos gadījumos sistēma ir uzskatāma par pamata drošības sistēmu.
8. Katra institūcija katrai sistēmai nodrošina šādu dokumentu izstrādi, izpildes uzraudzību un kontroli:
	1. sistēmas drošības politika;
	2. sistēmas drošības iekšējie noteikumi;
	3. sistēmas lietošanas noteikumi;
	4. sistēmas drošības riska pārvaldības plāns;
	5. sistēmas darbības atjaunošanas plāns.
9. Uz pamata drošības sistēmām nav attiecināmas prasības, kas minētas šo noteikumu 8.2., 8.3., 8.4., 8.5. apakšpunktā.
10. Šo noteikumu 8. punktā minētos dokumentus apstiprina institūcijas vadītājs. Institūcija visus šo noteikumu 8. punktā minētos dokumentus pārskata vismaz reizi gadā, kā arī šādos gadījumos:
	1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;
	2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;
	3. ja pēkšņi pieaug sistēmas drošības incidentu skaits vai noticis nozīmīgs sistēmas drošības incidents;
	4. ja izmaiņas institūcijas organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;
	5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.
11. Ja valsts institūcijas vai pašvaldības pārziņā vai turējumā ir vairāk nekā viena sistēma, katru no šo noteikumu 8. punktā minētajiem dokumentiem var izstrādāt vienoti vairākām vai visām pārziņā vai turējumā esošajām sistēmām, ja nepieciešams, norādot specifiskās prasības katrai sistēmai.
12. Sistēmas drošības pasākumu atbilstību šo noteikumu 5. punktā minētajām prasībām novērtē, pamatojoties uz sistēmas drošības pārbaudes rezultātiem. Ja šīs pārbaudes laikā konstatēti būtiski trūkumi, institūcija veic pasākumus to novēršanai atbilstoši Informācijas tehnoloģiju drošības likuma prasībām.

**II. Sistēmas drošības politika un iepirkumu prasības**

1. Sistēmas drošības politika ietver:
	1. sistēmas drošības politikas mērķus un pamatnostādnes;
	2. sistēmas raksturojumu un analīzi drošības jomā;
	3. sistēmas drošības pārvaldības organizācijas principus;
	4. sistēmas drošības atbilstību normatīvajiem aktiem un standartiem;
	5. sistēmas drošības principus, sistēmas drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamo līmeni atbilstoši šo noteikumu 7. punktā aprakstītajai metodikai un citus sistēmas drošības kritērijus (piemēram, sistēmas nepārtrauktās darbības laiks, sistēmas darbības atjaunošanas laiks, nosacījumi, pie kuriem ikdienas procedūras aizstājamas ar krīzes pārvaldības procedūrām).
2. Institūcija nodrošina, ka šo noteikumu 13.5. apakšpunktā minētā informācija ir pieejama sistēmas lietotājiem.
3. Izstrādājot sistēmas drošības politiku, tajā iekļauj prasības, kas paredz, ka:
	1. sistēmas lietotāji, kas veic sistēmas administrēšanas darbu, izmanto tam īpašus lietotāju kontus (turpmāk – sistēmas administratora konts), kas netiek izmantoti ikdienas darbību veikšanai;
	2. katrs lietotāja konts ir saistīts ar konkrētu fizisko personu; ja sistēmā tiek izmantoti konti, kas nav piesaistāmi konkrētai fiziskai personai (turpmāk – sistēmkonti), tad sistēmā jābūt iestrādātiem tehniskiem līdzekļiem, kas novērš iespēju lietotājiem izmantot sistēmkontus;
	3. ja sistēmā netiek izmantota daudzfaktoru autentifikācija, t.i., viens atribūts, kam nav statiska daba (piemēram, kodu kalkulators, vienreiz lietojams īsziņas kods), un vismaz viens cits atribūts, tad sistēmas lietotājiem ir obligāti jālieto paroles;
	4. sistēmas lietotāja paroļu garums nav mazāks par deviņiem simboliem un satur vismaz lielo latīņu alfabēta burtu, mazo latīņu alfabēta burtu, ciparu un speciālu simbolu;
	5. sistēmas lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, tajā skaitā lietotāja autentifikācijas procesa ietvaros, izņemot 15.7. apakšpunktā minēto;
	6. sistēmas lietotāja parole ievadīšanas brīdī lietotājam netiek pilnībā attēlota;
	7. sistēmas lietotāja parole, kas nosūtīta publiskā datu pārraides tīklā nešifrētā veidā, ir vienreiz lietojama un derīga ne ilgāk kā 72 stundas pēc tās nosūtīšanas;
	8. sistēmā nav pieļaujama funkcionalitāte, kas atļauj sistēmas lietotājam saglabāt savu paroli tā, lai tā turpmākajās pieslēgšanas reizēs nav jāievada;
	9. iekārtām, tajā skaitā infrastruktūras iekārtām, kas nodrošina sistēmas funkcionēšanu, netiek izmantotas noklusējuma (ražotāja vai izplatītāja uzstādītās) paroles;
	10. tiek nodrošināta sistēmas auditācijas pierakstu (turpmāk – sistēmas pieraksti) veidošana un uzglabāšana vismaz 6 mēnešus pēc ieraksta izdarīšanas;
	11. jebkura piekļuve sistēmai ir izsekojama līdz konkrētam sistēmas lietotāja kontam vai interneta protokola (IP) adresei;
	12. sistēmai jābūt uzliktiem visiem pieejamiem programmatūras atjauninājumiem, iepriekš izvērtējot to nepieciešamību;
	13. visās institūcijas valdījumā esošajās gala lietotāju iekārtās, kas ikdienā tiek izmantotas, lai pieslēgtos sistēmai, jābūt iekļautai pretvīrusu funkcionalitātei;
	14. sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām.
4. Sistēmas drošības politikā var paredzēt arī stingrākas drošības prasības, nekā noteikts šajos noteikumos, ciktāl tas nav pretrunā ar citiem normatīvajiem aktiem.
5. Pirms institūcija izstrādā vai uzsāk iepirkumu par jaunas sistēmas izstrādi, tā izstrādā un apstiprina šīs sistēmas drošības politiku un nodrošina, ka sistēmas izstrādes gaitā tā tiek ievērota.
6. Institūcija nodrošina, ka pirms jaunas sistēmas pieņemšanas ekspluatācijā, tai ir veikti ielaušanās testi. Ielaušanās testus veic tāda juridiska persona vai tādi institūcijas darbinieki, kas nav piedalījušies sistēmas izstrādē.
7. Institūcija nodrošina šo noteikumu 12. punktā minēto sistēmas drošības pārbaudi, vismaz reizi gadā veicot drošības dokumentācijas prasību īstenošanas pārbaudi.
8. Ja sistēmas uzturēšanai institūcija slēdz ārpakalpojuma līgumu ar pakalpojuma sniedzēju, tad līguma izpildi uzrauga atbildīgā persona un līgumā iekļauj drošības prasības, kas nav zemākas par šajos noteikumos noteikto, līgumā nosakot:
	1. saņemamā ārpakalpojuma aprakstu;
	2. precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;
	3. institūcijas un ārpakalpojuma sniedzēja tiesības un pienākumus, to skaitā:
		1. institūcijas tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti,
		2. institūcijas tiesības dot ārpakalpojuma sniedzējam obligāti izpildāmus norādījumus jautājumos, kas saistīti ar ārpakalpojuma godprātīgu, kvalitatīvu, savlaicīgu un normatīvajiem aktiem atbilstošu izpildi,
		3. institūcijas tiesības iesniegt ārpakalpojuma sniedzējam motivētu rakstveida pieprasījumu nekavējoties izbeigt ārpakalpojuma līgumu, ja institūcija konstatējusi, ka ārpakalpojumu sniedzējs nepilda ārpakalpojuma līgumā noteiktās prasības attiecībā uz ārpakalpojuma apjomu vai kvalitāti,
		4. ārpakalpojuma sniedzēja pienākumu nodrošināt institūcijai iespēju pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti.
9. Ja institūcija uzsāk iepirkumu par esošas sistēmas uzlabojumiem, tā nodrošina, ka atbilstošās drošības prasības tiek iekļautas iepirkuma specifikācijā.
10. Ja institūcija uzsāk iepirkumu par jaunas sistēmas izstrādi, tā iepirkuma specifikācijā iekļauj prasības, kas paredz:
	1. noteiktu sistēmas uzturēšanas un atbalsta nodrošināšanas (tajā skaitā sistēmas drošības nepilnību novēršanas) laika periodu;
	2. sistēmas datorprogrammu pirmkoda un tā izmantošanas tiesību nodošanu institūcijai ne vēlāk kā pēc šo noteikumu 22.1. apakšpunktā noteiktā laika perioda beigām, kā arī pēc katru izmaiņu vai uzlabojumu veikšanas tajā;
	3. iespēju šo noteikumu 22.1. apakšpunktā noteiktajā laika periodā turpināt sistēmas ekspluatēšanu ar jaunākām programmnodrošinājuma versijām, kas ir obligāti nepieciešams sistēmas funkcionēšanai (piemēram, operētājsistēma, datubāzu vadības sistēma, interpretators u.tml.).
11. Veicot iepirkumu par jaunas sistēmas izstrādi vai esošas sistēmas uzlabojumiem, institūcija iepirkuma specifikācijā iekļauj aizliegumu līgumā ierobežot Autortiesību likuma 29. panta pirmajā daļā noteiktās tiesības.

**III. Prasības paaugstinātas drošības sistēmām**

1. Izstrādājot sistēmas drošības politiku paaugstinātas drošības sistēmām, ņem vērā šo noteikumu 15. punkta prasības un papildus paredz, ka:
	1. katram sistēmas lietotājam parole ir obligāti jāmaina pēc ne vairāk kā 90 dienām, taču lietotājam aizliegts pašrocīgi mainīt paroli biežāk kā divas reizes 24 stundu laikā;
	2. sistēmas lietotāja parole jāizvēlas tā, lai tā nesakristu ne ar vienu no piecām iepriekšējām sistēmas lietotāja parolēm;
	3. piecas secīgas reizes nepareizi ievadot sistēmas lietotāja konta paroli, šis konts (izņemot sistēmas administratora kontu) nekavējoties tiek bloķēts;
	4. 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;
	5. fiziski piekļūt iekārtām, kas nodrošina sistēmas darbību, atļauts vienīgi iestādes pilnvarotām personām;
	6. tiek nodrošināta sistēmas pierakstu veidošana un uzglabāšana vismaz 18 mēnešus pēc ieraksta izdarīšanas, uzglabājot sistēmas pierakstus vai to kopijas atsevišķi no sistēmas;
	7. sistēmas pieraksti tiek veidoti, nodrošinot, ka tajos norādītais laiks sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC) ar vienas sekundes precizitāti;
	8. tiek nodrošināta sistēmas pierakstu satura plānveida uzraudzība un analīze, lai konstatētu incidentus;
	9. sistēmas lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju (t.i. tādu informāciju, kas nepieciešama, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu);
	10. plūsma starp sistēmu un tās lietotājiem, kā arī starp sistēmu un citām sistēmām tiek kontrolēta, piemēram, izmantojot ugunsmūri;
	11. datortīkla pakalpojumi (*network services*), kas netiek izmantoti sistēmas darbības nodrošināšanai, ir atslēgti;
	12. veicot sistēmas izstrādi un testēšanu, nav pieļaujams radīt apdraudējumu sistēmā glabāto datu integritātei;
	13. 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.
2. Iekšējie sistēmas drošības noteikumi nosaka:
	1. sistēmas informācijas resursu izveidošanas, papildināšanas, mainīšanas, apstrādes, pārraidīšanas, glabāšanas, atjaunošanas un iznīcināšanas kārtību;
	2. sistēmas informācijas un tehnisko resursu lietošanas un tās kontroles kārtību;
	3. kārtību, kādā tiek nodrošināta piekļūšana sistēmas informācijas un tehniskajiem resursiem;
	4. sistēmas informācijas resursu rezerves kopiju izgatavošanas un glabāšanas kārtību, kā arī kārtību, kādā pārbauda, vai ar sistēmas informācijas resursu rezerves kopijām iespējams atjaunot sistēmas informācijas resursus;
	5. datu nesēju lietošanas, pārvietošanas, glabāšanas un iznīcināšanas kārtību;
	6. kārtību, kādā lieto un glabā informāciju vai datus, kas nepieciešami, lai piekļūtu sistēmas informācijas un tehniskajiem resursiem;
	7. prasības sistēmas informācijas resursu aizsardzībai, kuru īsteno, izmantojot programmatūras līdzekļus (piemēram, sistēmas lietotāja atpazīšana un viņa pilnvaru atbilstības pārbaude attiecīgajām darbībām sistēmā, pasargājot sistēmas informācijas resursus no tīšas vai nejaušas bojāšanas vai iznīcināšanas);
	8. prasības sistēmas tehnisko resursu aizsardzībai pret fiziskas iedarbības radītu sistēmas drošības apdraudējumu (piemēram, ugunsgrēks, plūdi, sprieguma pazemināšanās vai pārspriegums enerģijas pievades tīklā, sistēmas tehnisko resursu zādzība, gaisa mitrums vai temperatūra, kas neatbilst ekspluatācijas noteikumiem);
	9. kārtību, kādā novēro sistēmas drošības apdraudējuma tuvošanās pazīmes;
	10. kārtību, kādā atklāj un pārvalda sistēmas drošības incidentus;
	11. kārtību, kādā sistēma darbojas, ja tās informācijas vai tehniskie resursi nav pieejami pilnā apjomā;
	12. kārtību, kādā maina sistēmas tehniskos resursus;
	13. institūcijas darbinieku apmācības un zināšanu pārbaudes kārtību sistēmas drošības jomā.
3. Sistēmas lietošanas noteikumi ietver:
	1. sistēmas lietotāju tiesības, pienākumus, ierobežojumus un atbildību;
	2. sistēmas lietotāju reģistrācijas un tās atcelšanas kārtību;
	3. sistēmas lietošanas kārtību;
	4. sistēmas lietotāju atbalsta kārtību.
4. Sistēmas drošības riska pārvaldības plāns ietver:
	1. veicamās risku analīzes metodoloģijas aprakstu;
	2. sistēmas drošības risku analīzi;
	3. pasākumus sistēmas drošības riska mazināšanai, to izpildes termiņus, finansējumu un par izpildi atbildīgo personu sarakstu.
5. Īstenojot sistēmas drošības riska pārvaldības plānu, nodrošina sistēmas drošības riska pieņemamo līmeni.
6. Sistēmas drošības riska pārvaldības plānu izstrādā un aktualizē, pamatojoties uz sistēmas drošības risku analīzi.
7. Sistēmas drošības risku analīze ietver:
	1. sistēmas drošības apdraudējumu uzskaitījumu, to īstenošanās varbūtības novērtējumu un tuvošanās pazīmju uzskaitījumu;
	2. institūcijas, sistēmas datu subjektu un sistēmas lietotāju iespējamo zaudējumu vai kaitējuma novērtējumu, ja notiktu sistēmas drošības incidents;
	3. sistēmas drošības riska novērtējumu;
	4. sistēmas drošības riska mazināšanas pasākumu un tajos izmantojamo līdzekļu uzskaitījumu;
	5. sistēmas drošības riska mazināšanai veikto pasākumu lietderības novērtējumu.
8. Sistēmas drošības riskus analizē savlaicīgi, ja sistēmā plāno izdarīt izmaiņas, kas ietekmē sistēmas drošību.
9. Institūcija nodrošina, lai sistēmas drošības riska mazināšanas pasākumos izmantojamie līdzekļi būtu samērojami ar iespējamiem zaudējumiem vai kaitējumu, kas institūcijai, sistēmas datu subjektiem un sistēmas lietotājiem varētu rasties sistēmas drošības incidenta dēļ.
10. Sistēmas darbības atjaunošanas plāns ietver:
	1. sistēmas informācijas un tehnisko resursu atjaunošanas pasākumus, kas veicami pēc sistēmas drošības incidenta;
	2. sistēmas darbības atjaunošanas pasākumu procedūru aprakstu;
	3. sistēmas darbības atjaunošanas pasākumos iesaistīto atbildīgo personu apziņošanas kārtību un darbības instrukcijas;
	4. atbildīgo personu apmācības, nodarbību un sagatavotības pārbaužu plānu.
11. Paaugstinātas drošības sistēmām, kas pieejamas, izmantojot publisku datu pārraides tīklu, institūcija nodrošina šo noteikumu 12. punktā minēto sistēmas drošības pārbaudi, vismaz reizi divos gados pasūtot ārēju drošības dokumentācijas auditu un ielaušanās testu veikšanu. Šo pakalpojumu iepirkumu centralizēti organizē Aizsardzības ministrija.
12. Pasūtot ārējas drošības pārbaudes veikšanu paaugstinātas drošības sistēmai, institūcija paredz, ka juridiska persona, kas veic auditu, ir reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, tās darbinieki, kas iesaistīti drošības audita veikšanā, ir NATO, Eiropas Savienības, Eiropas Ekonomikas zonas valstu pilsoņi vai Latvijas Republikas nepilsoņi, un juridiskā persona apstrādā audita laikā iegūto informāciju vienīgi NATO, Eiropas Savienības un Eiropas Ekonomikas zonas valstu teritorijā.
13. Paaugstinātas drošības sistēmu uzturēšanas ārpakalpojuma līgumu atļauts slēgt vienīgi ar juridisku personu, kas ir reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, vai fizisku personu, kas ir NATO, Eiropas Savienības, Eiropas Ekonomikas zonas valsts pilsonis vai Latvijas Republikas nepilsonis.

**IV. Noslēguma jautājumi**

1. Institūcijas šo noteikumu 8. punktā norādītos dokumentus apstiprina līdz 2017. gada 1. janvārim. Dokumenti, kas izstrādāti pirms šo noteikumu spēkā stāšanās, attiecībā uz valsts informāciju sistēmām paliek spēkā, ciktāl tie nav pretrunā ar šiem noteikumiem.
2. Attiecībā uz pamata drošības sistēmām, kas ir nodotas institūciju lietošanā līdz 2017. gada 1. janvārim, šo noteikumu 15. punkts ir spēkā no 2021. gada 1. janvāra.
3. Attiecībā uz paaugstinātas drošības sistēmām, kas ir nodotas institūciju lietošanā līdz 2017. gada 1. janvārim, šo noteikumu 15. un 24. punkts ir spēkā no 2018. gada 1. janvāra.
4. Sistēmu, kuras līdz šo noteikumu 38. un 39. punktā norādītajam attiecīgi 15. un 24. punkta spēkā stāšanās brīdim neatbilst minimālajām drošības prasībām, ekspluatēšanu pārtrauc viena gada laikā pēc attiecīgā punkta spēkā stāšanās, nodrošinot, ka sistēmas funkcijas nepieciešamības gadījumā pārņem tās pašas vai citas institūcijas sistēma.
5. Atzīt par spēku zaudējušiem Ministru kabineta 2005. gada 11. oktobra noteikumus Nr. 765 „Valsts informācijas sistēmu vispārējās drošības prasības” (Latvijas Vēstnesis, 2005, 164. nr.).

Ministru prezidente L.Straujuma

Aizsardzības ministrs R. Bergmanis

Iesniedzējs:

Aizsardzības ministrs R. Bergmanis

Vīza:

valsts sekretārs J. Sārts

09.07.2015. 17:00

2766

K.Solovjovs

67335037; kirils.solovjovs@mod.gov.lv