Izdevējs: Ministru kabinets
Veids: noteikumi
Numurs: 442
Pieņemts: 28.07.2015.
Stājas spēkā: 04.08.2015.

Publicēts:
Latvijas Vēstnesis, 149 (5467), 03.08.2015.
OP numurs: 2015/149.7

Attēlotā redakcija: 18.01.2019. - ...

Grozījumi:

MK 19.12.2017. noteikumi Nr.756 / LV, 254 (6081), 21.12.2017. / Stājas spēkā 01.01.2018.
MK 15.01.2019. noteikumi Nr.16 / LV, 12 (6351), 17.01.2019. / Stājas spēkā 18.01.2019.

Ministru kabineta noteikumi Nr. 442

Rīgā 2015. gada 28. jūlijā (prot. Nr. 36 63. §)

Kārtība, kādā tiek nodrošināta informācijas un komunikācijas tehnoloģiju sistēmu atbilstība minimālajām drošības prasībām

Izdoti saskaņā ar Informācijas tehnoloģiju drošības likuma 8. panta piekto un sesto daļu un Valsts informācijas sistēmu likuma 4. panta otro daļu
(Grozīta ar MK 15.01.2019. noteikumiem Nr. 16)

I. Vispārīgie jautājumi

1. Noteikumi nosaka:

1.1. valsts un pašvaldību institūciju informācijas un komunikācijas tehnoloģiju minimālās drošības prasības un kārtību, kādā valsts un pašvaldību institūcijas un informācijas tehnoloģiju kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji nodrošina informācijas un komunikācijas tehnoloģiju sistēmu atbilstību minimālajām prasībām;

1.2. valsts informācijas sistēmu vispārējās drošības prasības;

1.3. informācijas tehnoloģiju drošības prasības privāto tiesību juridiskajām personām, kas ir pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

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.

(Grozīts ar MK 19.12.2017. noteikumiem Nr. 756)

3. Noteikumi attiecas uz valsts un pašvaldību institūciju vai informācijas tehnoloģiju kritiskās infrastruktūras informācijas un komunikācijas tehnoloģiju sistēmām, tai skaitā valsts informācijas sistēmām (turpmāk – sistēmas), kas ir testēšanas stadijā, kā arī sistēmām, kas nodotas lietošanā. Citās sistēmas stadijās (plānošana, projektēšana, izstrāde) jānodrošina atbilstoša sistēmā esošas informācijas aizsardzība.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

4. Šajos noteikumos minētos par informācijas tehnoloģiju drošības pārvaldību atbildīgās personas pienākumus attiecībā uz valsts informācijas sistēmu veic sistēmas drošības pārvaldnieks, bet attiecībā uz informācijas tehnoloģiju kritisko infrastruktūru – par infrastruktūras drošību atbildīgā persona.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

4.[1] Valsts un pašvaldību institūcijas savā darbībā izmanto informācijas un komunikācijas tehnoloģijas, kas atbilst šajos noteikumos sistēmām noteiktajām prasībām, kā arī ņem vērā kompetentās valsts drošības iestādes un Informācijas tehnoloģiju drošības incidentu novēršanas institūcijas izstrādātos ieteikumus par izmantojamām informācijas un komunikācijas tehnoloģijām (tostarp par bezmaksas programmatūru un veicamajiem drošības pasākumiem).

(MK 15.01.2019. noteikumu Nr. 16 redakcijā)

4.[2] Privāto tiesību juridiskās personas, kas ir pamatpakalpojuma sniedzēji un digitālā pakalpojuma sniedzēji, ievēro šajos noteikumos sistēmām noteiktās prasības, ciktāl šajos noteikumos nav noteikts citādi.

(MK 15.01.2019. noteikumu Nr. 16 redakcijā)

5. Sistēmas drošībai īsteno pasākumu kopumu, lai:

5.1. nodrošinātu informācijas pieejamību (piekļuvi informācijai noteiktā laikposmā pēc informācijas pieprasīšanas);

5.2. nodrošinātu informācijas integritāti (pilnīgas un nemainītas informācijas saglabāšanu);

5.3. nodrošinātu informācijas konfidencialitāti (informācijas nodošanu tikai tām personām, kuras ir pilnvarotas to saņemt un lietot);

5.4. aizsargātu sistēmas informācijas resursus (datnes, arī tās, kuras satur sistēmā glabājamo, apstrādājamo un sistēmas lietotājiem pieejamo informāciju, un sistēmas dokumentāciju);

5.5. aizsargātu sistēmas tehniskos resursus (datorus, programmatūru, datu nesējus, datortīkla iekārtas un citas tehniskās iekārtas, kuras nodrošina sistēmas darbību);

5.6. 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);

5.7. novērtētu sistēmas drošības risku;

5.8. atklātu sistēmas drošības incidentu;

5.9. atjaunotu sistēmas darbību pēc sistēmas drošības incidenta.

6. Sistēmas iedala divās kategorijās – pamata un paaugstinātas drošības sistēmas.

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.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

7.[1] Kritiskās infrastruktūras informācijas sistēmas un sistēmas, ko izmanto pamatpakalpojuma vai digitālā pakalpojuma sniegšanai attiecīgi pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs, ir atzīstamas par paaugstinātas drošības sistēmām.

(MK 15.01.2019. noteikumu Nr. 16 redakcijā)

8. Valsts un pašvaldību institūcija, informācijas tehnoloģiju kritiskās infrastruktūras īpašnieks vai tiesiskais valdītājs, pamatpakalpojuma sniedzējs vai digitālā pakalpojuma sniedzējs (turpmāk – institūcija) izstrādā šādus dokumentus katrai sistēmai, kā arī nodrošina tajos noteikto prasību izpildes uzraudzību un kontroli:

8.1. sistēmas drošības politika;

8.2. sistēmas drošības iekšējie noteikumi;

8.3. sistēmas lietošanas noteikumi;

8.4. sistēmas drošības riska pārvaldības plāns;

8.5. sistēmas darbības atjaunošanas plāns.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

9. Uz pamata drošības sistēmām nav attiecināmas prasības, kas minētas šo noteikumu 8.2., 8.3., 8.4. un 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:

10.1. ja izmaiņas sistēmā var ietekmēt sistēmas drošību;

10.2. ja mainījušies vai ir atklāti jauni sistēmas drošības apdraudējumi;

10.3. ja pēkšņi pieaug sistēmas drošības incidentu skaits vai ir noticis nozīmīgs sistēmas drošības incidents;

10.4. ja izmaiņas institūcijas organizatoriskajā struktūrā skar sistēmas drošības vadības organizāciju;

10.5. ja izdarīti grozījumi normatīvajos aktos, kas regulē sistēmas darbību.

11. Ja institūcijas pārziņā vai turējumā ir vairāk nekā viena sistēma, katru šo noteikumu 8. punktā minēto dokumentu var izstrādāt vairākām vai visām pārziņā vai turējumā esošajām sistēmām vienotu, 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 likumā noteiktajām prasībām.

II. Sistēmas drošības politika un iepirkumu prasības

13. Sistēmas drošības politika ietver:

13.1. sistēmas drošības politikas mērķus un pamatnostādnes;

13.2. sistēmas raksturojumu un analīzi drošības jomā;

13.3. sistēmas drošības pārvaldības organizācijas principus;

13.4. sistēmas drošības atbilstību normatīvajiem aktiem un standartiem;

13.5. sistēmas drošības principus, sistēmas drošības risku (pieejamības, integritātes un konfidencialitātes risku) pieņemamo līmeni atbilstoši šo noteikumu 7. punktā minētajai 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).

14. Institūcija nodrošina, ka šo noteikumu 13.5. apakšpunktā minētā informācija ir pieejama reģistrētiem sistēmas lietotājiem.
(Grozīts ar MK 19.12.2017. noteikumiem Nr. 756)

15. Izstrādājot sistēmas drošības politiku, paredz, ka:

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

15.2. katrs reģistrēta 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 reģistrētiem lietotājiem izmantot sistēmkontus;

15.3. ja sistēmā netiek izmantota daudzfaktoru autentifikācija, tas ir, viens atribūts, kam nav statiska daba

(piemēram, kodu kalkulators, vienreiz lietojams īsziņas kods), un vismaz viens cits atribūts, tad reģistrētiem sistēmas lietotājiem obligāti jālieto paroles;

15.4. sistēmas lietotāja paroles garums nav mazāks par deviņām rakstu zīmēm un satur vismaz vienu lielo latīņu alfabēta burtu un mazo latīņu alfabēta burtu, kā arī ciparu vai speciālu simbolu;

15.5. sistēmas lietotāja paroles aizliegts elektroniski glabāt un transportēt nešifrētā veidā, arī lietotāja autentifikācijas procesa ietvaros, izņemot šo noteikumu 15.7. apakšpunktā minēto gadījumu;

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

15.7. 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;

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

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

15.10. tiek nodrošināta sistēmas auditācijas pierakstu (turpmāk – sistēmas pieraksti) veidošana un uzglabāšana vismaz sešus mēnešus pēc ieraksta izdarīšanas. Sistēmas pierakstos ietver informāciju par pieslēgšanos vai atslēgšanos no sistēmas, datu atlasi, kā arī konta izveidi, grozīšanu vai dzēšanu, fiksējot notikuma laiku, kas sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC), interneta protokola adresi, no kuras veikta darbība, aprakstu, kā arī informāciju par darbības iniciatoru – identifikatoru, pieslēguma metadatus;

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

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

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

15.14. sistēmas funkcionalitāte ir izpildāma ar minimāli iespējamām tiesībām.

(Grozīts ar MK 19.12.2017. noteikumiem Nr. 756; MK 15.01.2019. noteikumiem Nr. 16)

16. Sistēmas drošības politikā var paredzēt arī stingrākas drošības prasības, nekā noteikts šajos noteikumos, ciktāl tas nav pretrunā ar citiem normatīvajiem aktiem.

17. 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.

18. Institūcija nodrošina, ka pirms jaunas sistēmas pieņemšanas ekspluatācijā tai ir veikti ielaušanās testi. Ielaušanās testus veic juridiska persona vai institūcijas darbinieki, kuri nav piedalījušies sistēmas izstrādē.

19. Institūcija nodrošina šo noteikumu 12. punktā minēto sistēmas drošības pārbaudi, vismaz reizi gadā veicot drošības dokumentācijas prasību izpildes pārbaudi.

20. Ja institūcija sistēmas uzturēšanai slēdz ārpakalpojuma līgumu ar pakalpojuma sniedzēju, līguma izpildi uzrauga atbildīgā persona un līgumā iekļauj drošības prasības, kas nav zemākas par šajos noteikumos minētajām. Līgumā nosaka:

20.1. saņemamā ārpakalpojuma aprakstu;

20.2. precīzas prasības attiecībā uz ārpakalpojuma apjomu un kvalitāti;

20.3. institūcijas un ārpakalpojuma sniedzēja tiesības un pienākumus, tai skaitā:

20.3.1. institūcijas tiesības pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti;

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

20.3.3. institūcijas tiesības iesniegt ārpakalpojuma sniedzējam pamatotu rakstisku pieprasījumu nekavējoties izbeigt ārpakalpojuma līgumu, ja institūcija konstatējusi, ka ārpakalpojumu sniedzējs nepilda ārpakalpojuma līgumā noteiktās prasības attiecībā uz ārpakalpojuma apjomu vai kvalitāti;

20.3.4. ārpakalpojuma sniedzēja pienākumu nodrošināt institūcijai iespēju pastāvīgi uzraudzīt ārpakalpojuma sniegšanas kvalitāti.

21. Ja valsts un pašvaldību institūcija uzsāk iepirkumu par esošas sistēmas uzlabojumiem, tā nodrošina, ka atbilstošās drošības prasības tiek iekļautas iepirkuma specifikācijā.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

22. Ja valsts un pašvaldību institūcija uzsāk iepirkumu par jaunas sistēmas izstrādi, tā iepirkuma specifikācijā iekļauj prasības, paredzot:

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

22.2. sistēmas datorprogrammu pirmkoda un tā izmantošanas tiesību nodošanu institūcijai ne vēlāk kā pēc šo noteikumu 22.1. apakšpunktā noteiktā laikposma beigām, kā arī pēc katru izmaiņu vai uzlabojumu veikšanas tajā;

22.3. iespēju šo noteikumu 22.1. apakšpunktā noteiktajā laikposmā turpināt sistēmas ekspluatēšanu ar sistēmas funkcionēšanai obligāti nepieciešamā programmnodrošinājuma (piemēram, operētājsistēma, datubāzu vadības sistēma, interpretators) jaunākām versijām.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

23. Veicot iepirkumu par jaunas sistēmas izstrādi vai esošas sistēmas uzlabojumiem, valsts un pašvaldību institūcija iepirkuma specifikācijā iekļauj aizliegumu līgumā ierobežot Autortiesību likuma 29. panta pirmajā daļā noteiktās tiesības.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

III. Prasības paaugstinātas drošības sistēmām

24. Izstrādājot sistēmas drošības politiku paaugstinātas drošības sistēmām, ņem vērā šo noteikumu 15. punktā minētās prasības un papildus paredz, ka:

24.1. katram sistēmas lietotājam parole ir obligāti jāmaina ne vēlāk kā pēc 90 dienām, taču paroli aizliegts pašrocīgi mainīt biežāk nekā divas reizes 24 stundu laikā;

24.2. sistēmas lietotāja parole jāizvēlas tā, lai tā nesakristu ne ar vienu no piecām iepriekšējām sistēmas lietotāja parolēm;

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

24.4. 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;

24.5. fiziski piekļūt iekārtām, kas nodrošina sistēmas darbību, atļauts vienīgi iestādes pilnvarotām personām;

24.6. tiek nodrošināta sistēmas (gan servisa, gan operētājsistēmas) pierakstu veidošana (ietverot sistēmas auditācijas datus – autentifikācijas datus un tīkla plūsmas auditācijas datus, domēna vārdu sistēmas (DNS) servera pierakstus, ielaušanās atklāšanas sistēmu (IDS) pierakstus, operētājsistēmas autentifikācijas pierakstus) un uzglabāšana vismaz 18 mēnešus pēc ieraksta izdarīšanas, uzglabājot sistēmas pierakstus vai to kopijas atsevišķi – nodalīti no attiecīgās sistēmas;

24.7. sistēmas pieraksti tiek veidoti, nodrošinot, ka tajos norādītais laiks sakrīt ar faktiskā notikuma koordinēto pasaules laiku (UTC) ar vienas sekundes precizitāti;

24.8. tiek nodrošināta sistēmas pierakstu satura plānveida uzraudzība un analīze, lai konstatētu incidentus;

24.9. sistēmas lietotājiem redzamie kļūdu paziņojumi satur tikai minimāli nepieciešamo informāciju, lai sistēmas lietotājs pašrocīgi vai ar sistēmas atbalsta personāla palīdzību atrisinātu kļūdu;

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

24.11. datortīkla pakalpojumi (*network services*), kas netiek izmantoti sistēmas darbības nodrošināšanai, ir atslēgti;

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

24.13. 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.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

25. Iekšējie sistēmas drošības noteikumi nosaka:

25.1. sistēmas informācijas resursu izveidošanas, papildināšanas, mainīšanas, apstrādes, pārraidīšanas, glabāšanas, atjaunošanas un iznīcināšanas kārtību;

25.2. sistēmas informācijas un tehnisko resursu lietošanas un tās kontroles kārtību;

25.3. kārtību, kādā tiek nodrošināta piekļūšana sistēmas informācijas un tehniskajiem resursiem;

25.4. 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;

25.5. datu nesēju lietošanas, pārvietošanas, glabāšanas un iznīcināšanas kārtību;

25.6. kārtību, kādā lieto un glabā informāciju vai datus, kas nepieciešami, lai piekļūtu sistēmas informācijas un tehniskajiem resursiem;

25.7. 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);

25.8. 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);

25.9. kārtību, kādā novēro sistēmas drošības apdraudējuma tuvošanās pazīmes;

25.10. kārtību, kādā atklāj un pārvalda sistēmas drošības incidentus;

25.11. kārtību, kādā sistēma darbojas, ja sistēmas informācijas vai tehniskie resursi nav pieejami pilnā apjomā;

25.12. kārtību, kādā maina sistēmas tehniskos resursus;

25.13. institūcijas darbinieku apmācības un zināšanu pārbaudes kārtību sistēmas drošības jomā;

25.14. kārtību, kādā izvērtē ieviešamo sistēmas jauninājumu ietekmi uz sistēmu drošību;

25.15. kārtību, kādā veido, uzglabā, apstrādā un dzēš sistēmas pierakstu datnes.
(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

26. Sistēmas lietošanas noteikumi ietver:

26.1. sistēmas lietotāju tiesības, pienākumus, ierobežojumus un atbildību;

26.2. sistēmas lietotāju reģistrācijas un tās atcelšanas kārtību;

26.3. sistēmas lietošanas kārtību;

26.4. sistēmas lietotāju atbalsta kārtību.

27. Sistēmas drošības riska pārvaldības plāns ietver:

27.1. veicamās risku analīzes metodoloģijas aprakstu;

27.2. sistēmas drošības risku analīzi;

27.3. pasākumus sistēmas drošības riska mazināšanai, to izpildes termiņus, finansējumu un par izpildi atbildīgo personu sarakstu.

28. Īstenojot sistēmas drošības riska pārvaldības plānu, nodrošina sistēmas drošības riska pieņemamo līmeni.

29. Sistēmas drošības riska pārvaldības plānu izstrādā un aktualizē, pamatojoties uz sistēmas drošības risku analīzi.

30. Sistēmas drošības risku analīze ietver:

30.1. sistēmas drošības apdraudējumu uzskaitījumu, to īstenošanās varbūtības novērtējumu un tuvošanās pazīmju uzskaitījumu;

30.2. institūcijas, sistēmas datu subjektu un sistēmas lietotāju iespējamo zaudējumu vai kaitējuma novērtējumu, ja notiktu sistēmas drošības incidents;

30.3. sistēmas drošības riska novērtējumu;

30.4. sistēmas drošības riska mazināšanas pasākumu un tajos izmantojamo līdzekļu uzskaitījumu;

30.5. sistēmas drošības riska mazināšanai veikto pasākumu lietderības novērtējumu.

31. *(Svītrots ar MK 15.01.2019. noteikumiem Nr. 16)*

32. 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.

33. Sistēmas darbības atjaunošanas plāns ietver:

33.1. sistēmas informācijas un tehnisko resursu atjaunošanas pasākumus, kas veicami pēc sistēmas drošības incidenta;

33.2. sistēmas darbības atjaunošanas pasākumu procedūru aprakstu;

33.3. sistēmas darbības atjaunošanas pasākumos iesaistīto atbildīgo personu apziņošanas kārtību un darbības instrukcijas;

33.4. atbildīgo personu apmācības, nodarbību un sagatavotības pārbaužu plānu.

34. 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.

(Grozīts ar MK 19.12.2017. noteikumiem Nr. 756)

35. Pasūtot ārējas drošības pārbaudi 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.

36. 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.

36.[1] Līgumu par pakalpojumu, programmatūru vai iekārtu iegādi paaugstinātas drošības sistēmām atļauts slēgt ar juridisku personu, kas ir reģistrēta NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas dalībvalstī, vai fizisku personu, kas ir Latvijas Republikas valstspiederīgais, NATO, Eiropas Savienības vai Eiropas Ekonomikas zonas valsts pilsonis.

(MK 15.01.2019. noteikumu Nr. 16 redakcijā)

36.[2] Privāto tiesību juridiskās personas, kuras ir atzītas par pamatpakalpojuma sniedzējiem vai kuru īpašumā vai valdījumā esošās sistēmas ir atzītas par kritiskās infrastruktūras informācijas sistēmām, sešu mēnešu laikā no dienas, kad pieņemts lēmums par pamatpakalpojuma sniedzēja statusa piešķiršanu vai par atzīšanu par kritisko infrastruktūru, nodrošina, ka attiecīgās sistēmas atbilst šajos noteikumos noteiktajām prasībām.

(MK 15.01.2019. noteikumu Nr. 16 redakcijā)

IV. Noslēguma jautājumi

37. Atzīt par spēku zaudējušiem Ministru kabineta 2005. gada 11. oktobra noteikumus Nr. 765 " Valsts informācijas sistēmu vispārējās drošības prasības" (Latvijas Vēstnesis, 2005, 164. nr.; 2008, 195. nr.; 2009, 85. nr.; 2010, 150. nr.; 2011, 19. nr.).

38. Valsts un pašvaldību institūcijas šo noteikumu 8. punktā norādītos dokumentus apstiprina līdz 2017. gada 1. janvārim. Dokumenti, kas izstrādāti pirms šo noteikumu spēkā stāšanās, attiecībā uz valsts informācijas sistēmām paliek spēkā, ciktāl tie nav pretrunā ar šiem noteikumiem.

(Grozīts ar MK 15.01.2019. noteikumiem Nr. 16)

39. Attiecībā uz pamata drošības sistēmām, kas ir nodotas institūciju lietošanā līdz 2017. gada 1. janvārim, šo noteikumu 15. punktu piemēro no 2021. gada 1. janvāra.

40. Attiecībā uz paaugstinātas drošības sistēmām, kas ir nodotas institūciju lietošanā līdz 2017. gada 1. janvārim, šo noteikumu 15. un 24. punktu piemēro no 2018. gada 1. janvāra.

41. Ja sistēma līdz šo noteikumu 38. un 39. punktā norādītajai attiecīgi 15. un 24. punkta piemērošanas dienai neatbilst minimālajām drošības prasībām, tās ekspluatēšanu pārtrauc gada laikā pēc attiecīgajā punktā minētā piemērošanas datuma, nodrošinot, ka sistēmas funkcijas, ja nepieciešams, pārņem tās pašas vai citas institūcijas sistēma.

42. Ārējās drošības dokumentācijas auditu un ielaušanās testus šo noteikumu 34. punktā minētajām paaugstinātas drošības sistēmām, kas pieejamas, izmantojot publisku datu pārraides tīklu, institūcija nodrošina no 2019. gada 1. janvāra.

(MK 19.12.2017. noteikumu Nr. 756 redakcijā)

43. Privāto tiesību juridiskajām personām, kas ir informācijas tehnoloģiju kritiskās infrastruktūras īpašnieki vai tiesiskie valdītāji, pamatpakalpojuma sniedzēji un digitālo pakalpojumu sniedzēji, šo noteikumu prasības piemēro ar 2019. gada 1. maiju.

(MK 15.01.2019. noteikumu Nr. 16 redakcijā)

Informatīva atsauce uz Eiropas Savienības direktīvu

(MK 15.01.2019. noteikumu Nr. 16 redakcijā)

Noteikumos iekļautas tiesību normas, kas izriet no Eiropas Parlamenta un Padomes 2016. gada 6. jūlija Direktīvas (ES) 2016/1148 par pasākumiem nolūkā panākt vienādi augsta līmeņa tīklu un informācijas sistēmu drošību visā Savienībā.

Ministru prezidenta vietā –
satiksmes ministrs Anrijs Matīss

Aizsardzības ministrs Raimonds Bergmanis