Suvestinė redakcija nuo 2022-12-28

Įsakymas paskelbtas: TAR 2020-07-15, i. k. 2020-15796

VALSTYBĖS SIENOS APSAUGOS TARNYBOS PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VADAS

ĮSAKYMAS DĖL KAI KURIŲ VALSTYBĖS SIENOS APSAUGOS TARNYBOS PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ VALSTYBĖS IR KITŲ INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2020 m. liepos 15 d. Nr. 4-251
Vilnius

Vadovaudamasis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7.1 papunkčiu, 11, 12, 19, 26, 31 punktais bei Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, 6 punktu:

1. T v i r t i n u pridedamus Kai kurių Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos valdomų valstybės ir kitų informacinių sistemų duomenų saugos nuostatus (toliau – Saugos nuostatai).

2. S k i r i u Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – tarnyba) Informatikos skyriaus informacinių technologijų ir ryšių saugumo specialistą Saugos nuostatų priede nurodytų informacinių sistemų (toliau – informacinės sistemos) saugos įgaliotiniu (toliau – saugos įgaliotinis).

3. Į p a r e i g o j u saugos įgaliotinį:

3.1. ne vėliau kaip per 15 dienų nuo šio įsakymo įsigaliojimo dienos pateikti tarnybos vadui pasiūlymus dėl informacinių sistemų administratorių, duomenų valdymo įgaliotinio (-ių) ir kompetentingo asmens ar padalinio, atsakingo už informacinių sistemų kibernetinio saugumo organizavimą ir užtikrinimą, paskyrimo;

3.2. ne vėliau kaip per 6 mėnesius nuo šio įsakymo įsigaliojimo dienos parengti ir pateikti tarnybos vadui tvirtinti:

3.2.1. Informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles;

3.2.2. Informacinių sistemų naudotojų administravimo taisykles;

3.2.3. Informacinių sistemų veiklos tęstinumo planą.

4. P r i p a ž į s t u netekusiais galios:

4.1. tarnybos vado 2004 m. spalio 8 d. įsakymo Nr. 4-507 „Dėl Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos informacinės sistemos (VSATIS) nuostatų bei Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos informacinės sistemos (VSATIS) duomenų saugos nuostatų patvirtinimo“ 1.2 papunktį;

4.2. tarnybos vado 2012 m. liepos 30 d. įsakymo Nr. 4-552 „Dėl Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos Personalo tvarkymo taikomosios sistemos nuostatų patvirtinimo“ 1.2 papunktį;

4.3. tarnybos vado 2016 m. vasario 10 d. įsakymo Nr. 4-73 „Dėl Tarnybinės uniformos apskaitos informacinės sistemos aprašo ir Tarnybinės uniformos apskaitos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ 1.2, 2.1 papunkčius;

4.4. tarnybos vado 2016 m. gruodžio 7 d. įsakymo Nr. 4-575 „Dėl Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos 2016 m. vasario 10 d. įsakymo Nr. 4-73 „Dėl Tarnybinės uniformos apskaitos informacinės sistemos aprašo ir Tarnybinės uniformos apskaitos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo“ 1 punktą.

5. P a v e d u tarnybos struktūrinių padalinių vadovams Dokumentų valdymo sistemos „Kontora“ priemonėmis supažindinti su šiuo įsakymu pavaldžius valstybės tarnautojus ir darbuotojus, dirbančius pagal darbo sutartis.

6. N u s t a t a u, kad šis įsakymas skelbiamas tarnybos interneto svetainėje ir Teisės aktų registre.

Tarnybos vado pavaduotojas,
atliekantis tarnybos vado funkcijas Antanas Montvydas

SUDERINTA
Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos
2020 m. vasario 7 d. raštu Nr. (4.2 E) 6K-83

SUDERINTA
Informatikos ir ryšių departamento prie Lietuvos Respublikos vidaus reikalų ministerijos

PATVIRTINTA
Valstybės sienos apsaugos tarnybos prie
Lietuvos Respublikos vidaus reikalų ministerijos
vado 2020 m liepos 15 d. įsakymu Nr. 4-251

KAI KURIŲ VALSTYBĖS SIENOS APSAUGOS TARNYBOS PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ VALSTYBĖS IR KITŲ INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kai kurių Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos valdomų valstybės ir kitų informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) nustato Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Valstybės sienos apsaugos tarnyba) valdomų valstybės ir kitų informacinių sistemų (toliau – informacinės sistemos) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Saugos nuostatų reikalavimai taikomi tvarkant informacines sistemas, nurodytas Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos valdomų valstybės ir kitų informacinių sistemų sąraše (Saugos nuostatų priedas).

3. Elektroninės informacijos saugos ir kibernetinio saugumo politika įgyvendinama pagal Valstybės sienos apsaugos tarnybos vado tvirtinamus informacinių sistemų saugos politiką įgyvendinančius dokumentus: Saugaus elektroninės informacijos tvarkymo taisykles, Informacinių naudotojų administravimo taisykles, Informacinių sistemų veiklos tęstinumo valdymo planą ir kitus dokumentus, pagal kuriuos įgyvendinamos atskiros elektroninės informacijos saugos ir kibernetinio saugumo politikos nuostatos (toliau – saugos politiką įgyvendinantys dokumentai).

4. Saugos nuostatuose vartojamos sąvokos:

4.1. **informacinių sistemų komponentai** – kompiuterinės darbo vietos, tarnybinės stotys bei jose naudojamos operacinės sistemos, taikomųjų programų sistemos, duomenų saugyklos, duomenų bazės ir jų valdymo sistemos, kompiuterių tinklai, kompiuterių tinklo užkardos, įsilaužimų aptikimo ir prevencijos sistemos, elektroninio pašto valdymo sistema, kita techninė ir programinė įranga, kurios pagrindu funkcionuoja informacinės sistemos bei užtikrinama informacinėse sistemose tvarkomos elektroninės informacijos sauga;

4.2. **kibernetinio saugumo vadovas** – Valstybės sienos apsaugos tarnybos vado įsakymu paskirtas darbuotojas, atsakingas už informacinių sistemų kibernetinio saugumo politikos įgyvendinimo organizavimą ir priežiūrą; šias funkcijas atlikti gali būti pavesta Valstybės sienos apsaugos tarnybos struktūriniam padaliniui;

4.3. **saugos dokumentai** – informacinių sistemų duomenų saugos nuostatai ir saugos politiką įgyvendinantys dokumentai;

4.4. kitos Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrųjų saugos reikalavimų aprašas), Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo

įgyvendinimo“ (toliau – Kibernetinio saugumo reikalavimų aprašas), kituose Saugos nuostatų 27 punkte nurodytuose teisės aktuose ir standartuose apibrėžtas ir vartojamas sąvokas.

5. Informacinių sistemų elektroninės informacijos saugos ir kibernetinio saugumo (toliau – elektroninės informacijos sauga) užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

5.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

5.3. užtikrinti nuoseklų ir veiksmingą elektroninės informacijos saugos incidentų valdymą.

6. Informacinių sistemų elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

6.1. prieigos prie elektroninės informacijos ir jos tvarkymo priemonių ribojimas ir stebėsena;

6.2. elektroninės informacijos tvarkymo ir jos naudojimo stebėsena;

6.3. informacinių sistemų veiklos tęstinumo užtikrinimas;

6.4. informacinėse sistemose tvarkomų asmens duomenų apsauga;

6.5. iniciatyvi elektroninės informacijos saugos incidentų prevencija;

6.6. organizacinių, techninių, programinių, teisinių, informacijos sklaidos ir kitų priemonių, skirtų elektroninės informacijos saugai užtikrinti, įgyvendinimas ir kontrolė;

6.7. informacinių sistemų administratorių ir naudotojų mokymas elektroninės informacijos saugos klausimais.

7. saugos dokumentų taikymas ir naudojimas:

7.1. saugos dokumentai taikomi:

7.1.1. informacinių sistemų valdytojai ir tvarkytojai – Valstybės sienos apsaugos tarnybai, Savanorių pr. 2, Vilnius;

7.1.2. Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos informacinės sistemos (VSATIS) ir Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos Nacionalinio koordinacinio centro informacinės sistemos (toliau – kartu ISG) tvarkytojui – Informatikos ir ryšių departamentui prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Informatikos ir ryšių departamentas), Šventaragio g. 2, Vilnius;

7.1.3. kitiems informacinių sistemų tvarkytojams, nurodytiems informacinių sistemų nuostatuose;

7.1.4. Valstybės sienos apsaugos tarnybos paskirtam saugos įgaliotiniui;

7.1.5. kibernetinio saugumo vadovui;

7.1.6. informacinių sistemų duomenų valdymo įgaliotiniui;

7.1.7. Valstybės sienos apsaugos tarnybos paskirtiems informacinių sistemų administratoriams;

7.1.8. informacinių sistemų naudotojams;

7.1.9. informacinėse sistemose tvarkomų duomenų gavėjams, gaunantiems duomenis pagal nuolatinio duomenų teikimo sutartis;

7.1.10. paslaugų, susijusių su informacinėmis sistemomis, teikėjams;

7.2. saugos dokumentų naudojimo nuostatos:

7.2.1. Saugos nuostatai yra vieši;

7.2.2. saugos politiką įgyvendinantys dokumentai saugiai platinami ir prieinami su jais teisę susipažinti turinčioms valstybės institucijoms, kitoms suinteresuotoms šalims elektroninės informacijos saugos incidentų ar kibernetinio saugumo krizių atvejais;

7.2.3. informacinių sistemų naudotojams, paslaugų, susijusių su informacinėmis sistemomis, teikėjams ir kitiems tretiesiems asmenims suteikiama teisė susipažinti su saugos politiką įgyvendinančių dokumentų santraukomis;

7.3. už saugos politiką įgyvendinančių dokumentų santraukų, kurios turi būti sudaromos vadovaujantis principu „būtina žinoti“, parengimą atsakingas informacinių sistemų saugos įgaliotinis.

8. Už elektroninės informacijos saugą pagal kompetenciją atsako informacinių sistemų valdytoja ir tvarkytojai.

9. Valstybės sienos apsaugos tarnyba, kaip informacinių sistemų valdytoja, atsako už informacinių sistemų elektroninės informacijos saugos politikos formavimą, jos įgyvendinimo organizavimą ir priežiūrą, elektroninės informacijos ir duomenų tvarkymo bei duomenų teikimo duomenų gavėjams teisėtumą.

10. Informacinių sistemų duomenų valdymo įgaliotinis tiesiogiai atsako, kad informacinėse sistemose tvarkoma elektroninė informacija, duomenys, dokumentai ir (arba) jų kopijos būtų teikiami, skelbiami ir (arba) perduodami pagal teisės aktuose nustatytus reikalavimus.

11. Informacinių sistemų naudotojai, tvarkantys duomenis, informaciją, dokumentus ir (arba) jų kopijas, paslaugų ir paslaugų, susijusių su informacinėmis sistemomis, teikėjai privalo įsipareigoti saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir nutraukus su duomenų tvarkymu ar paslaugų teikimu susijusią veiklą.

12. Duomenų gavėjai, gaunantys informacinių sistemų duomenis ir informaciją pagal duomenų nuolatinio teikimo sutartis, atsako už administracinių, organizacinių ir techninių priemonių, atitinkančių gaunamos elektroninės informacijos svarbos lygį ir užtikrinančių jos saugą, įgyvendinimą.

13. Valstybės sienos apsaugos tarnyba, kaip informacinių sistemų valdytoja, atlieka informacinių sistemų nuostatuose nustatytas funkcijas, taip pat:

13.1. tvirtina saugos dokumentus;

13.2. prižiūri ir kontroliuoja, kad informacinės sistemos būtų tvarkomos vadovaujantis saugos dokumentais ir kitais elektroninės informacijos saugą reglamentuojančiais teisės aktais;

13.3. vertina techninės bei programinės įrangos priežiūros paslaugas teikiančių paslaugų teikėjų (jei tokie yra), veikiančių Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka, paslaugas, vykdo paslaugų teikėjų veiklos priežiūrą;

13.4. skiria saugos įgaliotinį, kibernetinio saugumo vadovą, informacinių sistemų administratorius;

13.5. priima sprendimus dėl:

13.5.1. techninių ir programinių priemonių, būtinų elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

13.5.2. informacinių sistemų rizikos ir informacinių technologijų saugos atitikties vertinimo atlikimo;

13.5.3. elektroninės informacijos saugos priemonių finansavimo;

13.6. tvirtina informacinių sistemų rizikos įvertinimo ir rizikos valdymo priemonių planą, informacinių technologijų saugos atitikties vertinimo metu nustatytų trūkumų šalinimo planą. Esant poreikiui, šie planai gali būti sujungti ir tvirtinamas bendras planas;

13.7. nagrinėja pasiūlymus dėl informacinių sistemų elektroninės informacijos saugos priemonių tobulinimo ir priima dėl jų sprendimus;

13.8. atlieka kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše bei kituose elektroninės informacijos saugos ir kibernetinio saugumo politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

14. Valstybės sienos apsaugos tarnyba, kaip informacinių sistemų tvarkytoja, atlieka informacinių sistemų nuostatuose nustatytas funkcijas, taip pat:

14.1. užtikrina tinkamą Saugos nuostatų, saugos politiką įgyvendinančių dokumentų, kitų dokumentų, susijusių su elektroninės informacijos sauga, įgyvendinimą;

14.2. užtikrina nepertraukiamą informacinių sistemų veikimą;

14.3. užtikrina informacinių sistemų sąveiką su kitomis valstybės informacinėmis sistemomis ir registrais;

14.4. užtikrina elektroninės informacijos, esančios informacinių sistemų duomenų bazėse, saugą;

14.5. užtikrina saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

14.6. įgyvendina priemones, mažinančias duomenų atskleidimo ir praradimo riziką bei užtikrinančias prarastų duomenų atkūrimą ir duomenų apsaugą nuo klastojimo;

14.7. rengia informacinių sistemų rizikos įvertinimo ir rizikos valdymo priemonių planą ir informacinių technologijų saugos atitikties vertinimo metu nustatytų trūkumų šalinimo planą. Esant poreikiui, šie planai gali būti sujungti ir rengiamas bendras planas;

14.8. vykdo kibernetinio saugumo organizavimo ir užtikrinimo funkcijas;

14.9. atlieka kitas Valstybės informacinių išteklių valdymo įstatyme, Kibernetinio saugumo įstatyme, Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

15. Informatikos ir ryšių departamentas, kaip ISG tvarkytojas, atlieka funkcijas, nustatytas ISG nuostatuose, šiuose Saugos nuostatuose, Informacinių technologijų ir telekomunikacijų paslaugų teikimo sutartyse ir kituose ISG valdytojo priimtuose teisės aktuose, reglamentuojančiuose ISG saugą (jie turi būti suderinti su Informatikos ir ryšių departamentu).

16. Kiti informacinių sistemų tvarkytojai užtikrina tvarkytojo įstaigoje tvarkomos informacinių sistemų elektroninės informacijos saugą, saugos dokumentuose nustatyta tvarka atsako už reikiamų organizacinių ir techninių saugos priemonių įgyvendinimą ir laikymąsi, taip pat turi šias teises bei pareigas ir atlieka šias funkcijas:

16.1. užtikrina tinkamą Valstybės sienos apsaugos tarnybos priimtų teisės aktų ir rekomendacijų, susijusių su elektroninės informacijos sauga, įgyvendinimą;

16.2. užtikrina tvarkytojo įstaigos informacinių sistemų naudotojų darbo vietose naudojamų administracinių, techninių ir programinių priemonių, užtikrinančių elektroninės informacijos saugą, diegimo koordinavimą ir priežiūrą;

16.3. pagal kompetenciją atsako už informacinių sistemų elektroninės informacijos tvarkymo teisėtumą;

16.4. užtikrina, kad tvarkytojo įstaigos darbuotojai, kurie yra informacinių sistemų naudotojai, būtų susipažinę su saugos dokumentais ir įsipareigoję saugoti informacinėse sistemose tvarkomų duomenų ir informacijos paslaptį;

16.5. valdo tvarkytojo įstaigos informacinių sistemų kompiuterinių darbo vietų saugos incidentus, saugos dokumentuose nustatyta tvarka informuoja apie juos Valstybės sienos apsaugos tarnybą ir kitas atsakingas institucijas, šalina šiuos incidentus;

16.6. teikia pasiūlymus Valstybės sienos apsaugos tarnybai dėl informacinių sistemų saugos tobulinimo;

16.7. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose bei saugos dokumentuose nustatytas funkcijas.

17. Valstybės sienos apsaugos tarnybos vadovo paskirtas saugos įgaliotinis atlieka šias funkcijas:

17.1. teikia Valstybės sienos apsaugos tarnybos vadovui pasiūlymus dėl:

17.1.1. administratoriaus (administratorių) skyrimo, reikalavimų administratoriui (administratoriams) nustatymo ir kibernetinio saugumo vadovo skyrimo;

17.1.2. informacinių technologijų saugos atitikties vertinimo;

Papunkčio pakeitimai:
Nr. 4-423, 2022-12-27, paskelbta TAR 2022-12-27, i. k. 2022-26989

17.1.3. saugos dokumentų priėmimo ir keitimo;

17.2. koordinuoja elektroninės informacijos saugos incidentų tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, elektroninės informacijos saugos incidentus, neteisėtas veikas, susijusias su saugos incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka kibernetinio saugumo vadovas;

17.3. teikia informacinių sistemų administratoriams ir informacinių sistemų naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos ir kibernetinio saugumo politikos įgyvendinimo;

17.4. derina paslaugų, susijusių su informacinėmis sistemomis, pirkimo ir informacinių sistemų duomenų teikimo sutartis;

17.5. organizuoja informacinių sistemų rizikos ir informacinių technologijų saugos atitikties vertinimą;

17.6. organizuoja informacinių sistemų naudotojams ir administratoriams mokomuosius ir pažintinius kursus informacinių sistemų elektroninės informacijos saugos klausimais;

17.7. atlieka kitas informacinių sistemų nuostatuose, Bendrųjų saugos reikalavimų apraše ir kituose teisės aktuose saugos įgaliotiniui priskirtas funkcijas.

18. Kibernetinio saugumo vadovas atlieka šias funkcijas:

18.1. analizuoja informacinių sistemų kibernetinio saugumo būklę, kylančių grėsmių, rizikos ir pažeidžiamų vietų vertinimą;

18.2. teikia informacinių sistemų administratoriams privalomus vykdyti nurodymus ir pavedimus dėl kibernetinio saugumo įgyvendinimo;

18.3. teikia informaciją ir pranešimus Nacionaliniam kibernetinio saugumo centrui apie:

18.3.1. įvykusius kibernetinio saugumo incidentus;

18.3.2. kibernetinių incidentų vertinimą;

18.3.3. didelės ir vidutinės reikšmės kibernetinių incidentų suvaldymą ar pasibaigimą;

18.4. atlieka kitas kibernetinio saugumo įgyvendinimo dokumentuose ir kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, kibernetinio saugumo vadovui priskirtas funkcijas.

19. Kibernetinio saugumo vadovu ir saugos įgaliotiniu gali būti tas pats asmuo.

20. Saugos įgaliotinis ir kibernetinio saugumo vadovas negali atlikti informacinių sistemų administratoriaus funkcijų.

21. Informacinių sistemų administratoriai gali būti skiriami vienai ar kelioms Valstybės sienos apsaugos tarnybos valdomoms informacinėms sistemoms, posistemiams, funkciškai

savarankiškoms sudedamosioms dalims ar kitoms konkrečioms informacinių sistemų administratoriaus funkcijoms atlikti.

22. Valstybės sienos apsaugos tarnybos skiriami informacinių sistemų administratoriai:

22.1. koordinuojantis administratorius – siekdamas užtikrinti tinkamą informacinių sistemų administratorių funkcijų vykdymą, koordinuoja ir prižiūri kitų Valstybės sienos apsaugos tarnybos paskirtų informacinių sistemų administratorių veiklą;

22.2. informacinių sistemų naudotojų administratoriai – atlieka naudotojų administravimo funkcijas:

22.2.1. registruoja ir išregistruoja informacinių sistemų naudotojus, tvarko esamų naudotojų duomenis;

22.2.2. pagal kompetenciją tvarko informacinių sistemų klasifikatorius;

22.2.3. stebi ir analizuoja informacinių sistemų naudotojų veiksmų įrašų žurnalus;

22.2.4. saugos dokumentuose nustatyta tvarka reaguoja į naudotojų veiksmus, pažeidžiančius saugos dokumentuose nustatytus reikalavimus;

22.3. informacinių sistemų komponentų administratoriai – atlieka funkcijas, susijusias su informacinių sistemų komponentais ir jų sąranka:

22.3.1. techninės informacinių sistemų infrastruktūros administratoriai, kurie atlieka funkcijas, susijusias su Valstybės sienos apsaugos tarnybos valdomos informacinių sistemų infrastruktūros komponentais ir jų sąranka:

22.3.1.1. administruoja Valstybės sienos apsaugos tarnybos kompiuterių tinklą:

22.3.1.1.1. užtikrina kompiuterių tinklo veikimą ir saugumą;

22.3.1.1.2. diegia, konfigūruoja ir prižiūri kompiuterių tinklo aktyviąją įrangą;

22.3.1.1.3. konfigūruoja įgaliotosios tarnybinės stoties bei interneto prieigos sąranką;

22.3.1.1.4. užtikrina duomenų apsikeitimą su kitomis valstybės informacinėmis sistemomis ir valstybės registrais;

22.3.1.1.5. aktyvių katalogų sistemoje (angl. *Microsoft Active Directory)* registruoja ir išregistruoja informacinių sistemų naudotojus, tvarko esamų naudotojų duomenis, nustato saugos politikas bei naudotojų ir naudotojų grupių prieigos prie informacinių sistemų teises;

22.3.1.1.6. atlieka informacinių sistemų naudojamos elektroninio pašto sistemos palaikymo ir priežiūros funkcijas;

22.3.1.1.7. vykdo kompiuterių tinklo perimetro stebėseną;

22.3.1.1.8. atlieka funkcijas, susijusias su kompiuterių tinklo pažeidžiamų vietų nustatymu, saugos reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus ir jų valdymu;

22.3.1.2. administruoja Valstybės sienos apsaugos tarnybos administracijos ir vietinių struktūrinių padalinių (pasienio rinktinės ir kt.) kompiuterių tinklus:

22.3.1.2.1. užtikrina vietinių kompiuterių tinklų veikimą ir saugumą;

22.3.1.2.2. diegia, konfigūruoja ir prižiūri vietinių kompiuterių tinklo aktyviąją įrangą;

22.3.1.2.3. konfigūruoja vietinių kompiuterių tinklų prieigą prie Valstybės sienos apsaugos tarnybos kompiuterių tinklo;

22.3.1.2.4. atlieka funkcijas, susijusias su vietinių kompiuterių tinklų pažeidžiamų vietų nustatymu, saugos reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos incidentus ir jų valdymu;

22.3.1.3. administruoja tarnybines stotis:

22.3.1.3.1. užtikrina tarnybinių stočių veikimą ir saugumą;

22.3.1.3.2. konfigūruoja tarnybinių stočių tinklo prieigą;

22.3.1.3.3. kuria ir administruoja tarnybinių stočių naudotojų registracijos duomenis;

22.3.1.3.4. stebi ir analizuoja tarnybinių stočių veiklą;

22.3.1.3.5. kuria ir atkuria tarnybinių stočių sąrankos ir jose saugomų bylų atsargines kopijas;

22.3.1.3.6. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

22.3.1.3.7. diegia tarnybinių stočių programinės įrangos atnaujinimus;

22.3.1.4. administruoja duomenų bazes:

22.3.1.4.1. užtikrina duomenų bazių veikimą ir saugumą;

22.3.1.4.2. tvarko duomenų bazių programinę įrangą;

22.3.1.4.3. kuria ir administruoja duomenų bazių naudotojų registracijos duomenis;

22.3.1.4.4. kuria ir atkuria duomenų bazių atsargines kopijas;

22.3.1.4.5. stebi duomenų bazes ir optimizuoja jų veikimą;

22.3.2. kompiuterinių darbo vietų administratoriai, kurie atlieka funkcijas, susijusias su informacinių sistemų naudotojų kompiuterines darbo vietas sudarančiais komponentais ir jų sąranka:

22.3.2.1. užtikrina kompiuterinių darbo vietų veikimą;

22.3.2.2. diegia ir konfigūruoja kompiuterinių darbo vietų sisteminę ir taikomąją programinę įrangą ir jos atnaujinimus;

22.3.2.3. užtikrina, kad kompiuterinėse darbo vietose būtų diegiama ir naudojama tik į Valstybės sienos apsaugos tarnybos vadovo tvirtinamą leistinos naudoti programinės įrangos sąrašą įtraukta programinė įranga;

22.3.2.4. atlieka funkcijas, susijusias su kompiuterinėse darbo vietose tvarkomos elektroninės informacijos saugos užtikrinimu, kenkėjiškos programinės įrangos aptikimu ir prevencija;

22.3.2.5. registruoja ir valdo su kompiuterinėmis darbo vietomis susijusius elektroninės informacijos saugos incidentus, informuoja apie juos saugos įgaliotinį ir koordinuojantį administratorių, teikia pasiūlymus dėl minėtų incidentų pašalinimo;

22.3.2.6. koordinuojančio administratoriaus pavedimu atlieka kitų informacinių sistemų komponentų administravimo funkcijas;

22.3.3. kitų informacinių sistemų komponentų administratoriai atlieka funkcijas, susijusias su kitų, Saugos nuostatų 4.1 papunktyje nurodytų, komponentų sąranka, veikimo stebėsena ir analize, profilaktine priežiūra, programinės įrangos diegimu ir konfigūravimu, trikdžių diagnostika ir šalinimu, nepertraukiamo informacinių sistemų veikimo užtikrinimu, pasiūlymų dėl jų veikimo optimizavimo teikimu;

22.4. saugos administratorius atlieka informacinių sistemų pažeidžiamų vietų nustatymo, saugumo reikalavimų atitikties nustatymo ir stebėsenos funkcijas.

23. Informacinių sistemų administratoriai yra atsakingi už tinkamą saugos dokumentuose ir pareigybių aprašymuose jiems priskirtų funkcijų vykdymą.

24. Informacinių sistemų administratoriai privalo:

24.1. pagal saugos dokumentuose ir pareigybių aprašymuose priskirtą kompetenciją reaguoti į elektroninės informacijos saugos incidentus;

24.2. atlikdami informacinių sistemų sąrankos pakeitimus, laikytis informacinių sistemų pokyčių valdymo tvarkos, nustatytos Informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse;

24.3. patikrinti (peržiūrėti) jiems priskirtų informacinių sistemų komponentų sąranką ir informacinių sistemų komponentų būsenos rodiklius ne rečiau kaip kartą per metus ir (arba) po informacinių sistemų pokyčių;

24.4. nuolat teikti saugos įgaliotiniui ir kibernetinio saugumo vadovui informaciją apie elektroninės informacijos saugą užtikrinančių informacinių sistemų komponentų būklę;

24.5. pagal kompetenciją dalyvauti atliekant informacinių technologijų saugos atitikties vertinimą bei informacinių sistemų rizikos vertinimą.

25. Informacinių sistemų administratoriai ir naudotojai privalo vykdyti visus saugos įgaliotinio ir kibernetinio saugumo vadovo nurodymus bei pavedimus dėl informacinių sistemų elektroninės informacijos saugos užtikrinimo.

26. Informacinių sistemų naudotojai privalo:

26.1. laikytis informacijos saugos ir kibernetinio saugumo reikalavimų, nustatytų Saugos nuostatuose, Saugos nuostatų 3 punkte nurodytuose saugos politiką įgyvendinančiuose dokumentuose, Saugos nuostatų 27 punkte nurodytuose teisės aktuose, reglamentuojančiuose informacijos saugą, kibernetinį saugumą ir asmens duomenų apsaugą;

26.2. pastebėję saugos dokumentuose nustatytų reikalavimų pažeidimų ar nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, galimus ar įvykusius kibernetinio saugumo incidentus, privalo nedelsdami pranešti apie tai informacinių sistemų saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka;

26.3. vykdyti informacinių sistemų administratorių nurodymus;

26.4. naudoti informacinius išteklius tik darbo ir tarnybinėms funkcijoms vykdyti;

26.5. naudoti tarnybinį elektroninį paštą tik tarnybiniam susirašinėjimui, susijusiam su darbu, tarnybinių pareigų ir funkcijų vykdymu;

26.6. saugoti savo slaptažodį, kitus prisijungimo prie informacinių sistemų duomenis ir priemones, neatskleisti slaptažodžio kitiems asmenims;

26.7. įtarę, kad prisijungimo prie informacinės sistemos slaptažodis galėjo būti atskleistas kitam asmeniui, praradę ar kitaip netekę slaptažodžio, nedelsdami imtis Informacinių sistemų naudotojų administravimo taisyklėse nustatytų veiksmų; nurodytais atvejais slaptažodis turi būti nedelsiant pakeistas Informacinių sistemų naudotojų administravimo taisyklių nustatyta tvarka.

Punkto pakeitimai:
Nr. 4-423, 2022-12-27, paskelbta TAR 2022-12-27, i. k. 2022-26989

27. Teisės aktai ir standartai, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugą:

27.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

27.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

27.3. Lietuvos Respublikos elektroninių ryšių įstatymas;

27.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

27.5. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo, kuriuo panaikinama Direktyva 95/46/EB (OL 2016 L 119, p. 1);

27.5[1]. 2017 m. lapkričio 30 d. Europos Parlamento ir Tarybos reglamentas (ES) 2017/2226, kuriuo sukuriama Atvykimo–išvykimo sistema (AIS), kurioje registruojami trečiųjų šalių piliečių, kertančių valstybių narių išorės sienas, atvykimo ir išvykimo bei atsisakymo leisti jiems atvykti duomenys, nustatomos prieigos prie AIS teisėsaugos tikslais sąlygos ir iš dalies keičiama Konvencija dėl Šengeno susitarimo įgyvendinimo ir reglamentai (EB) Nr. 767/2008 ir (ES) Nr. 1077/2011;

Papildyta papunkčiu:
Nr. 4-423, 2022-12-27, paskelbta TAR 2022-12-27, i. k. 2022-26989

27.6. Bendrųjų saugos reikalavimų aprašas;

27.7. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas (toliau – Techniniai elektroninės informacijos saugos reikalavimai) ir Informacinių technologijų atitikties vertinimo metodika (toliau – Informacinių technologijų atitikties vertinimo metodika), patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų

informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų atitikties vertinimo metodikos patvirtinimo;
Papunkčio pakeitimai:
Nr. 4-423, 2022-12-27, paskelbta TAR 2022-12-27, i. k. 2022-26989

27.8. Kibernetinio saugumo reikalavimų aprašas;

27.9. Valstybės sienos apsaugos tarnybos vado įsakymu patvirtintas Kibernetinių incidentų valdymo planas;

27.10. Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos informacinės sistemos (VSATIS) nuostatai, patvirtinti Valstybės sienos apsaugos tarnybos vado 2004 m. spalio 8 d. įsakymu Nr. 4-507 „Dėl Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos informacinės sistemos (VSATIS) nuostatų bei Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos informacinės sistemos (VSATIS) duomenų saugos nuostatų patvirtinimo“;

27.11. Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos tarnybinės uniformos apskaitos informacinės sistemos aprašas, patvirtintas Valstybės sienos apsaugos tarnybos vado 2016 m. vasario 10 d. įsakymu Nr. 4-73 „Dėl Tarnybinės uniformos apskaitos informacinės sistemos aprašo ir Tarnybinės uniformos apskaitos informacinės sistemos duomenų saugos nuostatų patvirtinimo“;

27.12. Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos personalo tvarkymo taikomosios sistemos nuostatai, patvirtinti Valstybės sienos apsaugos tarnybos vado 2012 m. liepos 30 d. įsakymu Nr. 4-552 „Dėl Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos Personalo tvarkymo taikomosios sistemos nuostatų patvirtinimo“;

27.13. Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos dokumentų valdymo sistemos nuostatai, patvirtinti Valstybės sienos apsaugos tarnybos vado 2019 m. spalio 14 d. įsakymu Nr. 4-448 „Dėl Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos vado 2009 m. birželio 5 d. įsakymo Nr. 4-389 „Dėl Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos Dokumentų valdymo sistemos nuostatų patvirtinimo“ pakeitimo“;

27.14. Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos Nacionalinio koordinacinio centro informacinės sistemos nuostatai, patvirtinti Valstybės sienos apsaugos tarnybos vado 2020 m. birželio 12 d. įsakymu Nr. 4-219 „Dėl Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos Nacionalinio koordinacinio centro informacinės sistemos steigimo ir jos nuostatų patvirtinimo“;

27.15. Asmens duomenų tvarkymo ir asmens duomenų subjektų teisių įgyvendinimo Valstybės sienos apsaugos tarnyboje prie Lietuvos Respublikos vidaus reikalų ministerijos tvarkos aprašas, patvirtintas Valstybės sienos apsaugos tarnybos vado 2019 m. vasario 8 d. įsakymu Nr. 4-52 „Dėl Asmens duomenų tvarkymo ir asmens duomenų subjektų teisių įgyvendinimo Valstybės sienos apsaugos tarnyboje prie Lietuvos Respublikos vidaus reikalų ministerijos tvarkos aprašo patvirtinimo“;

27.16. Lietuvos standartai LST EN ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST EN ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, kiti Lietuvos ir tarptautiniai „Informacijos technologijos. Saugumo metodai“ grupės standartai, nustatantys elektroninės informacijos saugos valdymą;

27.17. kiti teisės aktai, reglamentuojantys elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

28. Informacinėse sistemose tvarkomos elektroninės informacijos svarbos kategorijos, informacinių sistemų kategorijos ir informacinių sistemų priskyrimo kategorijoms kriterijai, nustatyti vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Klasifikavimo gairių aprašas), nurodyti Saugos nuostatų priede.

29. Saugos įgaliotinis, atsižvelgdamas į Lietuvos Respublikos vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius grupės „Informacijos technologija. Saugumo technika“ standartus, kasmet, jei teisės aktai nenustato kitaip, organizuoja informacinių sistemų rizikos įvertinimą. Prireikus, saugos įgaliotinis gali organizuoti neeilinį informacinių sistemų rizikos vertinimą. Informacinių sistemų valdytojos rašytiniu pavedimu informacinių sistemų rizikos vertinimą gali atlikti pats saugos įgaliotinis.

30. Informacinių sistemų rizikos vertinimas atliekamas Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos (toliau – ARSIS) priemonėmis.

31. Informacinių sistemų rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri pateikiama informacinių sistemų valdytojos vadovui. Rizikos įvertinimo ataskaita rengiama įvertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai yra šie:

31.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingos elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, elektroninės informacijos perdavimo tinklais triktys, programinės įrangos klaidos, netinkamas veikimas ir kita);

31.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacinėmis sistemomis elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, vagystės ir kita);

31.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 840 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

32. Atsižvelgdama į rizikos vertinimo ataskaitą, informacinių sistemų valdytoja, prireikus, tvirtina Informacinių sistemų rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame taip pat numatomas ir techninių, administracinių, organizacinių bei kitų išteklių poreikis rizikos valdymo gerinimo priemonėms įgyvendinti.

33. Rizikos įvertinimo ataskaitos ir rizikos valdymo priemonių plano kopijas informacinių sistemų valdytoja, ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo, pateikia ARSIS Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“ (toliau – ARSIS nuostatai), nustatyta tvarka.

34. Kartu su informacinių sistemų rizikos vertinimu atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinių sistemų kibernetiniam saugumui, rizikos vertinimas, kuris organizuojamas ir atliekamas Kibernetinio saugumo reikalavimų apraše nustatyta tvarka. Prireikus,

rengiamas rizikos vertinimo metu nustatytų Kibernetinio saugumo rizikų valdymo priemonių planas, kurį tvirtina informacinių sistemų valdytojos vadovas. Kibernetinio rizikų valdymo priemonių plane turi būti numatomas techninių, administracinių, organizacinių, kvalifikacijos tobulinimo bei kitų išteklių poreikis rizikos valdymo gerinimo priemonėms įgyvendinti.

35. Siekiant užtikrinti saugos dokumentuose nustatytų elektroninės informacijos saugos reikalavimų įgyvendinimo organizavimą ir kontrolę, turi būti organizuojamas informacinių sistemų informacinių technologijų saugos atitikties vertinimas. Informacinių technologijų saugos atitikties vertinimas turi būti atliekamas ne rečiau kaip kartą per dvejus metus, jei kiti teisės aktai nenustato kitaip.

36. Informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu gali būti atliekamas kibernetinių atakų imitavimas ir vykdomos kibernetinių incidentų imitavimo pratybos. Imituojant kibernetines atakas rekomenduojama vadovautis tarptautiniu mastu pripažintų organizacijų (pvz., EC-COUNCIL, ISACA, NIST ir kt.) rekomendacijomis ir gerąja praktika.

37. Informacinių technologijų atitikties vertinimas atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka.

Punkto pakeitimai:
Nr. 4-423, 2022-12-27, paskelbta TAR 2022-12-27, i. k. 2022-26989

38. Atlikus informacinių technologijų saugos atitikties vertinimą, saugos įgaliotinis rengia ir teikia informacinių sistemų valdytojos vadovui informacinių technologijų saugos vertinimo ataskaitą. Atsižvelgdamas į informacinių technologijų saugos atitikties vertinimo ataskaitą, saugos įgaliotinis, prireikus, parengia nustatytų trūkumų šalinimo planą, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato informacinių sistemų valdytojos vadovas.

39. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas informacinių sistemų valdytoja, ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo dienos, pateikia ARSIS, ARSIS nuostatuose nustatyta tvarka.

40. Elektroninės informacijos saugos būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis informacinių sistemų elektroninės informacijos saugos priemonėmis, jas parenkant vadovaujantis šiais pagrindiniais principais:

40.1. saugos priemonės turi būti valdomos centralizuotai;

40.2. saugos priemonių diegimo kaina turi būti adekvati saugomos informacijos vertei;

40.3. likutinė rizika turi būti sumažinta iki priimtino lygio;

40.4. kur galima, būtina įdiegti prevencines informacijos saugos priemones.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

41. Programinės įrangos, skirtos informacinėms sistemoms apsaugoti nuo kenksmingos programinės įrangos, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

41.1. informacinių sistemų naudojamose tarnybinėse stotyse ir informacinių sistemų naudotojų kompiuteriuose turi būti naudojamos ir centralizuotai valdomos kenksmingos programinės įrangos aptikimo ir blokavimo realiu laiku priemonės;

41.2. Saugos nuostatų 41.1 papunktyje nurodytos priemonės automatiškai turi informuoti informacinių sistemų komponentų administratorius apie tai, kuriems informacinės sistemos posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas;

41.3. informacinių sistemų komponentai, be kenksmingos programinės įrangos aptikimo ir blokavimo priemonių, gali būti eksploatuojami, jeigu informacinių sistemų rizikos vertinimo metu patvirtinama, kad šių komponentų rizika yra priimtina;

41.4. kenksmingos programinės įrangos aptikimo ir blokavimo priemonės turi atsinaujinti ne rečiau kaip kartą per 24 valandas;

41.5. kenksmingos programinės įrangos aptikimo priemonių sąrankos konfigūravimas turi būti apsaugotas slaptažodžiu.

42. Programinės įrangos, įdiegtos kompiuterinėse darbo vietose ir tarnybinėse stotyse, naudojimo nuostatos:

42.1. informacinių sistemų naudotojų kompiuterinėse darbo vietose ir informacinių sistemų naudojamose tarnybinėse stotyse turi būti naudojama tik teisėta programinė įranga;

42.2. kompiuterinėse darbo vietose naudojama programinė įranga turi būti įtraukta į informacinių sistemų valdytojos vadovo patvirtintą leistinos naudoti programinės įrangos sąrašą; leistinos naudoti programinės įrangos sąrašą turi parengti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti saugos įgaliotinis;

42.3. tarnybinių stočių ir kompiuterinių darbo vietų operacinių sistemų, elektroninės informacijos saugai užtikrinti naudojamų priemonių ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai bei klaidų pataisymai turi būti operatyviai išbandomi ir įdiegiami;

42.4. informacinių sistemų saugos administratorius ne rečiau kaip kartą per savaitę turi įvertinti informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir su atnaujinimais susijusius saugos pažeidžiamumo svarbos lygius informacinių sistemų posistemiuose, funkciškai savarankiškose informacinių sistemų sudedamosiose dalyse, kompiuterinėse darbo vietose ir apie įvertinimo rezultatus informuoti saugos įgaliotinį ir kibernetinio saugumo vadovą;

42.5. programinė įranga turi būti prižiūrima ir atnaujinama laikantis gamintojų reikalavimų ir rekomendacijų;

42.6. programinės įrangos diegimą, konfigūravimą, priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai – informacinių sistemų komponentų administratoriai arba tokias paslaugas teikiantys kvalifikuoti paslaugų teikėjai;

42.7. informacinių sistemų programinė įranga turi turėti apsaugą nuo pagrindinių per kompiuterių tinklus vykdomų atakų: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų atakų. Pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project* (*OWASP*) interneto svetainėje *www.owasp.org*;

42.8. elektroninės informacijos saugos priemonių sąranka turi būti konfigūruojama vadovaujantis šių priemonių gamintojų rekomendacijomis.

43. Programinės įrangos kūrimo ir testavimo nuostatos:

43.1. programinės įrangos kūrimas ir testavimas turi būti atliekamas aplinkoje, atskirtoje nuo informacinių sistemų gamybinės aplinkos;

43.2. testuojant programinę įrangą turi būti naudojami nuasmeninti duomenų rinkiniai; tais atvejais, kai testavimui naudojamuose duomenų rinkiniuose neįmanoma panaikinti galimybės nustatyti asmens tapatybę, turi būti naudojamos specialios asmens duomenų apsaugos užtikrinimo priemonės ar (ir) procedūros.

44. Kompiuterių tinklo filtravimo įrangos pagrindinės saugos valdymo nuostatos:

44.1. kompiuterių tinklai turi būti atskirti nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant užkardas, automatinę įsilaužimų aptikimo ir prevencijos įrangą, atkirtimo nuo paslaugos, dedikuoto atkirtimo nuo paslaugos įrangą;

44.2. kompiuterių tinklų perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešuose ryšių tinkluose naršančių vidinių informacinių sistemų naudotojų

kompiuterinę įrangą nuo kenksmingo kodo; visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingos programinės įrangos;

44.3. apsaugai nuo elektroninės informacijos neteisėto atskleidimo turi būti naudojama duomenų srautų analizės ir kontrolės įranga;

44.4. turi būti naudojamos turinio filtravimo sistemos;

44.5. turi būti naudojamos taikomųjų programų kontrolės sistemos.

45. **Belaidžio tinklo saugumo valdymo pagrindiniai reikalavimai:**

45.1. leidžiama naudoti tik su asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ar užtikrinimą, suderintus belaidės prieigos taškus ir belaidės prieigos įrenginius;

45.2. belaidės prieigos taškai gali būti diegiami tik atskiruose potinkliuose, kontroliuojamose zonose;

45.3. turi būti vykdoma belaidžių įrenginių kontrolė, tikrinama, ar eksploatuojami belaidžiai įrenginiai atitinka **techninius kibernetinio saugumo reikalavimus;**

45.4. **turi būti n**audojamos priemonės, kurios automatiškai apribotų neleistinus ar kibernetinio saugumo reikalavimų neatitinkančius belaidžius **įrenginius;**

45.5. prisijungiant prie belaidžio tinklo, turi būti taikomas informacinių sistemų naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas bei uždrausta belaidėje sąsajoje naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą;

45.6. **belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu.**

46. Interneto svetainių, naudojamų prisijungti prie Valstybės sienos apsaugos tarnybos valdomų informacinių sistemų ir pasiekiamų iš viešųjų elektroninių ryšių tinklų (toliau – svetainės), pagrindinės saugos valdymo nuostatos:

Punkto pakeitimai:

Nr. 4-423, 2022-12-27, paskelbta TAR 2022-12-27, i. k. 2022-26989

46.1. svetainių užkardos turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų (toliau – TVS) būtų galima jungtis tik iš vidinio informacinių sistemų tvarkytojos kompiuterinio tinklo arba nustatytų IP (angl. *Internet Protocol*) adresų;

46.2. turi būti pakeistos gamintojo numatytos prisijungimo prie svetainių TVS ir administravimo skydų (angl. *Panel*) nuorodos (angl. *Default path*) bei slaptažodžiai;

46.3. turi būti užtikrinama, kad prie svetainių TVS ir administravimo skydų būtų galima jungtis tik naudojantis šifruotu ryšiu;

46.4. svetainės turi atitikti kitus saugumo reikalavimus, nustatytus Techniniuose elektroninės informacijos saugos reikalavimuose, Kibernetinio saugumo reikalavimų apraše, Informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse;

46.5. svetainių saugumas turi būti vertinamas informacinių sistemų rizikos įvertinimo metu ir (arba) informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu, atliekamų Saugos nuostatų II skyriuje nustatyta tvarka.

47. Stacionarius kompiuterius leidžiama naudoti tik informacinių sistemų valdytojos ir informacinių sistemų tvarkytojų patalpose teisės aktuose nustatytoms informacinių sistemų naudotojų funkcijoms atlikti.

48. Leistinos nešiojamųjų kompiuterių ir mobiliųjų įrenginių (išmaniųjų telefonų ir planšetinių kompiuterių, naudojančių *Android* ar *iOS* operacines sistemas) naudojimo ribos:

48.1. prisijungti prie informacinių sistemų leidžiama naudoti tik tarnybinius nešiojamuosius kompiuterius ir mobiliuosius įrenginius;

48.2. asmuo, kuris tarnybinį nešiojamąjį kompiuterį ar mobilųjį įrenginį naudoja prisijungti prie informacinių sistemų ar jų atskirų komponentų, neturi teisių valdyti jo sąrankos ir jame įdiegtos programinės įrangos;

48.3. nešiojamiesiems kompiuteriams ir mobiliesiems įrenginiams, išnešamiems iš informacinių sistemų valdytojos ar informacinių sistemų tvarkytojų patalpų, turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimai, papildomos priemonės asmens tapatumo nustatymui ir kt.);

48.4. prie nešiojamųjų kompiuterių ir mobiliųjų įrenginių gali būti jungiami tik informacinių sistemų naudotojų tarnybinėms funkcijoms atlikti reikalingi įrenginiai, įtraukti į informacinių sistemų valdytojos vadovo tvirtinamą leistinų jungti įrenginių sąrašą;

48.5. už nešiojamojo kompiuterio ar mobiliojo įrenginio fizinį saugumą ir jame tvarkomos elektroninės informacijos saugą teisės aktų nustatyta tvarka atsako asmuo, kuriam šis kompiuteris ar įrenginys yra skirtas.

49. Kompiuterinių darbo vietų valdymo pagrindinės nuostatos:

49.1. visos informacinių sistemų naudotojų kompiuterinės darbo vietos turi būti valdomos centralizuotai, naudojant aktyvių katalogų sistemos (angl. *Microsoft Active Directory)* ar kitas lygiavertes priemones;

49.2. aktyvių katalogų sistemoje kiekvienai kompiuterinei darbo vietai turi būti nustatyta politika, leidžianti kompiuterinės darbo vietos naudotojui atlikti tik tuos veiksmus, kurie būtini tarnybinėms funkcijoms vykdyti;

49.3. kompiuterinės darbo vietos naudotojas savo tapatybę turi patvirtinti slaptažodžiu arba kita tapatumo patvirtinimo priemone;

49.4. kompiuterinėse darbo vietose gali būti diegiama tik į informacinių sistemų valdytojos vadovo tvirtinamą leistinos naudoti programinės įrangos sąrašą įtraukta programinė įranga;

49.5. naudotojas neturi teisių valdyti kompiuterinės darbo vietos sąrankos ir diegti joje bet kokią programinę įrangą;

49.6. kompiuterinėse darbo vietose turi būti įdiegtos priemonės, leidžiančios riboti išorinių duomenų laikmenų (USB, CD/DVD ir kt.) naudojimą;

49.7. išorinių laikmenų naudojimo ribojimo ir kiti reikalavimai kompiuterinėms darbo vietoms nustatyti saugos politiką įgyvendinančiuose dokumentuose.

Papunkčio pakeitimai:
Nr. 4-423, 2022-12-27, paskelbta TAR 2022-12-27, i. k. 2022-26989

50. Elektroninės informacijos laikmenų valdymo ir saugaus naudojimo pagrindinės nuostatos:

50.1. išnešamose iš informacinių sistemų valdytojos ar informacinių sistemų tvarkytojų patalpų išorinėse duomenų laikmenose esanti nevieša elektroninė informacija turi būti šifruojama;

50.2. iš stacionariųjų ir nešiojamųjų kompiuterių ar elektroninės informacijos laikmenų, kurios perduodamos remonto ar techninės priežiūros paslaugų teikėjui arba nurašomos, turi būti neatkuriamai pašalinta visa nevieša elektroninė informacija.

51. Metodai, kuriais užtikrinamas saugus elektroninės informacijos teikimas ir (ar) gavimas:

51.1. elektroninė informacija automatiniu būdu turi būti teikiama ir (ar) gaunama tik pagal informacinių sistemų nuostatuose ir duomenų teikimo sutartyse nustatytas specifikacijas ir sąlygas;

51.2. tiesioginė prieiga prie informacinių sistemų elektroninės informacijos suteikiama tik registruotiems naudotojams, naudojant saugos politiką įgyvendinančiuose dokumentuose nustatytas

informacinių sistemų naudotojų autentifikavimo priemones (tapatybės patvirtinimas slaptažodžiu ar kitu būdu);

51.3. informacinių sistemų naudotojų, jų vykdytų užklausų ir peržiūrėtų užklausų rezultatų duomenys tvarkomi Vidaus reikalų informacinės sistemos centrinio duomenų banko naudotojų administravimo posistemėje Lietuvos Respublikos vidaus reikalų ministro 2005 m. kovo 9 d. įsakymo Nr. 1V-68 „Dėl Vidaus reikalų informacinės sistemos centrinio duomenų banko duomenų peržiūros taisyklių patvirtinimo“ nustatyta tvarka;

51.4. visa perduodama ir gaunama elektroninė informacija šifruojama;

51.5. elektroninė informacija perduodama ir gaunama automatiniu būdu naudojant TCP/IP, HTTPS protokolus realiuoju laiku arba asinchroniniu režimu, esant Saugos nuostatų 51.1 papunktyje nurodytoms sąlygoms;

51.6. elektroninei informacijai teikti ir (ar) gauti naudojamas saugus Vidaus reikalų telekomunikacinis tinklas, saugus valstybinis duomenų perdavimo tinklas ar kiti saugūs elektroninių ryšių tinklai;

51.7. nuotolinis prisijungimas prie informacinių sistemų galimas naudojant virtualų privatų tinklą (angl. *Virtual Private Network, VPN*) ir kitus saugiųjų jungimų protokolus (*SSL, HTTPS* ar lygiaverčius);

51.8. šifro raktų ilgiai, šifro raktų generavimo algoritmai, šifro raktų apsikeitimo protokolai, sertifikato parašo šifravimo algoritmai ir kiti šifravimo algoritmai turi būti nustatomi atsižvelgiant į Lietuvos ir tarptautinių organizacijų ir standartų rekomendacijas, Techninius elektroninės informacijos saugos reikalavimus bei Kibernetinio saugumo reikalavimų apraše nustatytus reikalavimus;

51.9. naudojamų šifravimo priemonių patikimumas vertinamas neeilinio arba kasmetinio informacinių sistemų rizikos vertinimo metu; šifravimo priemonės turi būti operatyviai keičiamos nustačius saugumo spragų šifravimo algoritmuose.

52. Pagrindiniai atsarginių elektroninės informacijos kopijų darymo ir atkūrimo reikalavimai:

52.1. atsarginės elektroninės informacijos kopijos turi būti daromos ir saugomos tokios apimties, kad informacinių sistemų veiklos sutrikimo, saugos incidento ar elektroninės informacijos vientisumo praradimo atvejais informacinių sistemų neveikimo laikotarpis nebūtų ilgesnis, nei taikoma konkrečioms informacinių sistemų svarbos kategorijoms, nurodytoms Saugos nuostatų priede, o elektroninės informacijos praradimas atitiktų priimtinumo kriterijus;

52.2. atsarginės elektroninės informacijos kopijos turi būti daromos automatiškai, bet ne rečiau kaip atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarkoje, nustatytoje Informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėse, nurodytais terminais;

52.3. elektroninė informacija kopijose turi būti užšifruota; šifravimo raktai turi būti saugomi atskirai nuo kopijų arba turi būti imtasi kitų priemonių, dėl kurių nebūtų galima neteisėtai atkurti elektroninės informacijos;

52.4. atsarginės elektroninės informacijos kopijos turi būti saugomos kitose patalpose, nei yra informacinių sistemų tarnybinės stotys ar įrenginys, kurio elektroninė informacija buvo nukopijuota, arba kitame pastate;

52.5. atsarginių elektroninės informacijos kopijų darymas turi būti fiksuojamas;

52.6. ne rečiau kaip kartą per pusmetį turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai;

52.7. patekimas į patalpas, kuriose saugomos atsarginės elektroninės informacijos kopijos, turi būti kontroliuojamas.

53. Turi būti užtikrintas elektroninės informacijos saugos incidentų, įvykusių informacinėse sistemose, registravimas, valdymas ir tyrimas Kibernetinio saugumo reikalavimų apraše ir Informacinių sistemų veiklos tęstinumo plane nustatyta tvarka.

54. Turi būti analizuojama ir vertinama įgyta incidentų valdymo patirtis, prireikus rengiamas ir informacinių sistemų valdytojos vadovo tvirtinamas informacinių sistemų elektroninės informacijos saugos incidentų valdymo gerinimo priemonių planas, kuriame numatomas techninių, administracinių, kvalifikacijos tobulinimo ir kitų išteklių poreikis incidentų valdymo gerinimo priemonėms įgyvendinti.

55. Pagal Nacionalinį kibernetinių incidentų valdymo planą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, ir Informacinių sistemų veiklos tęstinumo plane nustatyta tvarka turi būti:

55.1. pranešama Nacionaliniam kibernetinio saugumo centrui ir kitoms atsakingoms institucijoms pagal kompetenciją apie įvykusius kibernetinio saugumo incidentus, jų vertinimą, priskyrimą kibernetinių incidentų kategorijoms (didelio poveikio, vidutinio poveikio, nereikšmingi) ir suvaldymą;

55.2. periodiškai teikiamos ataskaitos Nacionaliniam kibernetinio saugumo centrui apie įvykusių didelio ir vidutinio poveikio incidentų valdymo būklę, pranešama apie incidentų suvaldymą ar pasibaigimą (incidentas laikomas suvaldytu ar pasibaigusiu, kai išnyksta incidento poveikis ir (ar) atkuriama įprasta informacinių sistemų veikla);

55.3. informacinių sistemų valdytojai įvertinus, kad ji negalės savarankiškai ištirti ar suvaldyti kibernetinio incidento per maksimaliai leistiną informacinės sistemos neveikimo laiką, nustatytą saugos politiką įgyvendinančiuose dokumentuose, ne vėliau kaip per dvidešimt keturias valandas nuo šių aplinkybių nustatymo kreipiamasi pagalbos į Nacionalinį kibernetinio saugumo centrą;

55.4. ne vėliau kaip per aštuonias valandas nuo kibernetinio incidento suvaldymo ar pasibaigimo informuojami informacinių sistemų teikiamų paslaugų gavėjai, jeigu kibernetinio incidento poveikis padarė arba gali ateityje padaryti žalos informacinių sistemų teikiamų paslaugų gavėjams.

56. Elektroninio pašto saugaus naudojimo pagrindinės nuostatos:

56.1. draudžiama tarnybinį elektroninį paštą naudoti asmeninėms reikmėms, o asmeninį elektroninį paštą naudoti tarnybinėms reikmėms;

56.2. elektroniniu paštu siunčiama neskirta viešai skelbti ar kita jautri elektroninė informacija (asmens duomenys ar kt.) turi būti šifruojama, siunčiamai elektroninei informacijai iššifruoti reikalingi duomenys gavėjui turi būti perduodami kitomis priemonėmis (telefonu, SMS žinute, susitikus ar pan.), o nesant galimybių tai padaryti ir įvertinus, kad rizika priimtina, – kitu elektroniniu laišku;

56.3. draudžiama elektroniniu paštu perduoti įslaptintą elektroninę informaciją;

56.4. kiti elektroninės informacijos saugos reikalavimai elektroninio pašto administratoriams ir naudotojams nustatyti saugos politiką įgyvendinančiuose dokumentuose.

Papunkčio pakeitimai:
Nr. 4-423, 2022-12-27, paskelbta TAR 2022-12-27, i. k. 2022-26989

57. Turi būti užtikrinta informacinių sistemų naudojamo interneto saugumas ir kontrolė. Informacinių sistemų valdytoja turi būti sudariusi sutartį (-is) su interneto paslaugų teikėju (-ais) dėl reagavimo į kibernetinius incidentus, interneto paslaugos sutrikimų registravimo, apsaugos nuo informacinių sistemų veiklos trikdymo taikymo (angl. *Denial of Service, DoS)*. Informacinių sistemų valdytoja interneto saugumo ir kontrolės užtikrinimo funkcijas gali pavesti atlikti informacinių sistemų tvarkytojui.

58. Informacinių sistemų valdytoja, pirkdama paslaugas ar įrangą, susijusią su informacinių sistemų projektavimu, kūrimu, diegimu, modernizavimu ir elektroninės informacijos saugos užtikrinimu, turi:

58.1. pirkimo dokumentuose iš anksto nustatyti, kad paslaugų teikėjas, darbų vykdytojas ar įrangos tiekėjas užtikrina atitiktį Kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams;

58.2. į paslaugų pirkimo sutartį įtraukti nuostatą, įpareigojančią paslaugų teikėjo darbuotojus pasirašyti konfidencialumo pasižadėjimą neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant paslaugų pirkimo sutartį, išskyrus tiek, kiek tai būtina sutarčiai vykdyti, taip pat nenaudoti konfidencialios informacijos asmeniniams ar trečiųjų asmenų poreikiams, laikantis principo, kad visa paslaugų teikėjui suteikta informacija (įskaitant informacinėse sistemose tvarkomą elektroninę informaciją) yra konfidenciali, išskyrus, kai raštu patvirtinama, kad tam tikra pateikta informacija nėra konfidenciali.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

59. Informacinių sistemų valdytojos paskirtas saugos įgaliotinis ir kibernetinio saugumo vadovas privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, turi būti susipažinęs ir savo darbe vadovautis Saugos nuostatų 27 punkte nurodytais teisės aktais, kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

60. Informacinių sistemų administratoriai privalo išmanyti pagrindinius elektroninės informacijos saugos ir saugaus darbo su duomenų perdavimo tinklais principus, atsižvelgiant į vykdomas funkcijas atitinkamai turėti sisteminių programinių priemonių administravimo ir priežiūros patirties, mokėti administruoti ir prižiūrėti duomenų bazes, gebėti užtikrinti techninės ir programinės įrangos nepertraukiamą funkcionavimą bei saugą, stebėti techninės ir programinės įrangos veikimą, atlikti techninės ir programinės įrangos profilaktinę priežiūrą, sutrikimų bei saugos incidentų diagnostiką ir šalinimą, turėti sisteminių programinių priemonių (operacinių sistemų) administravimo ir priežiūros patirties.

61. Saugos įgaliotiniu, administratoriumi ar kibernetinio saugumo vadovu negali būti skiriamas asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimą elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo nuobaudos paskyrimo praėję mažiau kaip vieneri metai.

62. Informacinių sistemų naudotojai privalo turėti pagrindinių darbo kompiuteriu ir taikomosiomis programomis įgūdžių, mokėti saugiai tvarkyti elektroninę informaciją.

63. Informacinių sistemų naudotojai ir administratoriai turi būti susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, taip pat pagal kompetenciją su kitais teisės aktais bei standartais, reglamentuojančiais elektroninės informacijos saugą.

64. Informacinių sistemų naudotojai, tvarkantys elektroninę informaciją, privalo įsipareigoti saugoti informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą bei valstybės tarnybos ar darbo santykius.

65. Informacinių sistemų naudotojai, atliekantys tarnybines funkcijas, susijusias su asmens duomenų tvarkymu bei teikimu, privalo pasirašytinai susipažinti su asmens duomenų tvarkymą ir apsaugą reglamentuojančiais teisės aktais ir atsakomybe už jų pažeidimą bei raštu įpareigoti saugoti asmens duomenų paslaptį. Asmens duomenų paslaptį informacinių sistemų naudotojai privalo

saugoti ir pasibaigus darbo (tarnybos) santykiams, per visą asmens duomenų teisinės apsaugos laiką, jeigu asmens duomenų apsaugą reglamentuojantys Europos Sąjungos ir Lietuvos Respublikos teisės aktai nenumato kitaip.

66. Informacinių sistemų naudotojų teisės, pareigos ir leistini elektroninės informacijos tvarkymo veiksmai nustatyti Informacinių sistemų naudotojų administravimo taisyklėse.

67. Informacinių sistemų valdytoja turi sudaryti sąlygas saugos įgaliotiniui, kibernetinio saugumo vadovui ir informacinių sistemų administratoriams nuolatos tobulinti kvalifikaciją pagal savo kompetenciją.

68. Informacinių sistemų naudotojams ne rečiau kaip kartą per kalendorinius metus turi būti rengiami elektroninės informacijos saugos mokymai, įvairiais būdais primenama apie saugos problematiką (pvz., priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės ir pan.). Saugos mokymus periodiškai pagal kompetenciją organizuoja saugos įgaliotinis, kibernetinio saugumo vadovas arba asmens duomenų apsaugos pareigūnas.

V SKYRIUS
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

69. Informacinių sistemų naudotojų, administratorių ir kitų asmenų supažindinimą su Saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais ar jų santraukomis, atsakomybe už saugos dokumentų nuostatų pažeidimus organizuoja saugos įgaliotinis. Supažindinimo su saugos dokumentais ar jų santrauka būdai pasirenkami atsižvelgiant į informacinių sistemų specifiką (pvz., informacinių sistemų ir jų naudotojų buvimo vietą, organizacinių ar techninių priemonių, leidžiančių identifikuoti su saugos dokumentais ar jų santrauka susipažinusį asmenį ir užtikrinančių supažindinimo procedūros įrodomąją (teisinę) galią, panaudojimo galimybes ir pan.).

70. Pakartotinai su saugos dokumentais ar jų santrauka informacinių sistemų naudotojai ir administratoriai supažindinami tik iš esmės pasikeitus informacinėms sistemoms, saugos dokumentams ar kitiems elektroninės informacijos saugą reglamentuojantiems teisės aktams.

71. Tvarkyti informacinių sistemų elektroninę informaciją ar administruoti informacines sistemas gali tik tie asmenys, kurie yra susipažinę su saugos dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugą, taip pat su atsakomybe už saugos dokumentų nuostatų pažeidimus, ir sutikę laikytis saugos dokumentuose nustatytų reikalavimų.

72. Informacinių sistemų naudotojai, administratoriai, saugos įgaliotinis ir kiti asmenys, pažeidę saugos dokumentų nuostatas, atsako Lietuvos Respublikos ir Europos Sąjungos teisės aktų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

73. Informacinių sistemų valdytoja saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Keičiami saugos dokumentai turi būti derinami su Nacionaliniu kibernetinio saugumo centru prie Lietuvos Respublikos krašto apsaugos ministerijos, išskyrus atvejus, kai keičiant saugos dokumentus atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos nekeičiantys pakeitimai arba taisoma teisės technika.

74. Saugos dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) po to, kai atliekamas rizikos įvertinimas ar informacinių technologijų saugos atitikties vertinimas arba įvykus esminiams teisiniams, organizaciniams, sisteminiams ar kitiems su informacinių sistemų veikla susijusiems pokyčiams.

75. Bendrųjų saugos reikalavimų apraše nustatyta tvarka patvirtintų saugos dokumentų ar jų pakeitimų kopijos turi būti pateikiamos Registrų ir informacinių sistemų registrui ir Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos informacinei sistemai.

_____

Kai kurių Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos valdomų valstybės ir kitų informacinių sistemų duomenų saugos nuostatų priedas

VALSTYBĖS SIENOS APSAUGOS TARNYBOS PRIE LIETUVOS RESPUBLIKOS VIDAUS REIKALŲ MINISTERIJOS VALDOMŲ VALSTYBĖS IR KITŲ INFORMACINIŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	Informacinės sistemos pavadinimas	Informacinės sistemos trumpas pavadinimas	Informacinės sistemos elektroninės informacijos svarbos kategorija	Informacinės sistemos kategorija	Informacinės sistemos priskyrimo kategorijai kriterijai
1.	Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos informacinė sistema (VSATIS)	VSATIS	Svarbi	Antra	Klasifikavimo gairių aprašo 8.1, 8.3, 8.5, 8.6 ir 12.2 papunkčiai
2.	Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos tarnybinės uniformos aprūpinimo informacinė sistema	Tarnybinės uniformos aprūpinimo informacinė sistema	Mažiausios svarbos	Ketvirta	Klasifikavimo gairių aprašo 10 punktas ir 12.4 papunktis
3.	Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos personalo tvarkymo taikomoji sistema	Personalo tvarkymo taikomoji sistema	Mažiausios svarbos	Ketvirta	Klasifikavimo gairių aprašo 10 punktas ir 12.4 papunktis
4.	Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos dokumentų valdymo sistema	Dokumentų valdymo sistema	Mažiausios svarbos	Ketvirta	Klasifikavimo gairių aprašo 10 punktas ir 12.4 papunktis

5.	Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos Nacionalinio koordinacinio centro informacinė sistema	Nacionalinio koordinacinio centro informacinė sistema	Mažiausios svarbos	Ketvirta	Klasifikavimo gairių aprašo 10 punktas ir 12.4 papunktis

Pakeitimai:

1.
Valstybės sienos apsaugos tarnyba prie Lietuvos Respublikos vidaus reikalų ministerijos, Įsakymas
Nr. 4-423, 2022-12-27, paskelbta TAR 2022-12-27, i. k. 2022-26989
Dėl Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos vado 2020 m. liepos 15 d. įsakymo Nr. 4-251 „Dėl Kai kurių Valstybės sienos apsaugos tarnybos prie Lietuvos Respublikos vidaus reikalų ministerijos valdomų valstybės ir kitų informacinių sistemų duomenų saugos nuostatų patvirtinimo“ pakeitimo