VALSTYBINĖS TERITORIJŲ PLANAVIMO IR STATYBOS INSPEKCIJOS PRIE APLINKOS MINISTERIJOS VIRŠININKAS

ĮSAKYMAS DĖL KAI KURIŲ VALSTYBINĖS TERITORIJŲ PLANAVIMO IR STATYBOS INSPEKCIJOS PRIE APLINKOS MINISTERIJOS VALDOMŲ VALSTYBĖS IR KITŲ INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO IR SAUGOS ĮGALIOTINIO PASKYRIMO

2019 m. birželio 27 d. Nr. 1V-96
Vilnius

Vadovaudamasi 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, 11 ir 19 punktais:

1. T v i r t i n u Kai kurių Valstybinės teritorijų planavimo ir statybos inspekcijos prie Aplinkos ministerijos valdomų valstybės ir kitų informacinių sistemų duomenų saugos nuostatus (pridedama).

2. S k i r i u Valstybinės teritorijų planavimo ir statybos inspekcijos prie Aplinkos ministerijos (toliau – Inspekcija) Informacinių technologijų skyriaus (toliau – Skyrius) specialistą Jaunių Krivicką – Kai kurių Valstybinės teritorijų planavimo ir statybos inspekcijos prie Aplinkos ministerijos valdomų valstybės ir kitų informacinių sistemų duomenų saugos nuostatų (toliau – Saugos nuostatai) priede nurodytų informacinių sistemų saugos įgaliotiniu.

3. P a v e d u Skyriaus vedėjui užtikrinti, kad ne vėliau kaip per 3 mėnesius nuo Saugos nuostatų patvirtinimo dienos būtų parengtos, teisės aktų nustatyta tvarka suderintos ir Inspekcijos viršininkui tvirtinti pateiktos Saugos nuostatų priede nurodytų informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės, veiklos tęstinumo valdymo planas ir naudotojų administravimo taisyklės.

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

4.1. Inspekcijos viršininko 2014 m. vasario 13 d. įsakymą Nr. 1V-32 „Dėl Lietuvos Respublikos teritorijų planavimo dokumentų rengimo ir teritorijų planavimo proceso valstybinės priežiūros informacinės sistemos duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais;

4.2. Inspekcijos viršininko 2016 gegužės 17 d. įsakymą Nr. 1V-55 „Dėl Lietuvos Respublikos statybos leidimų ir statybos valstybinės priežiūros informacinės sistemos „Infostatyba“ duomenų saugos nuostatų patvirtinimo ir saugos įgaliotinio skyrimo“ su visais pakeitimais ir papildymais.

L. e. viršininko pareigas Renata Planutienė

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2019 m. birželio 5 d. raštu Nr. (4.2.) 6K-386

PATVIRTINTA
Valstybinės teritorijų planavimo ir statybos
inspekcijos prie Aplinkos ministerijos viršininko
2019 m. birželio 27 d. įsakymu Nr. 1V-96

KAI KURIŲ VALSTYBINĖS TERITORIJŲ PLANAVIMO IR STATYBOS INSPEKCIJOS PRIE APLINKOS MINISTERIJOS VALDOMŲ VALSTYBĖS IR KITŲ INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kai kurių Valstybinės teritorijų planavimo ir statybos inspekcijos prie Aplinkos ministerijos (toliau – Inspekcija) valdomų valstybės ir kitų informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Inspekcijos valdomų bei automatiniu būdu tvarkomų valstybės ir kitų informacinių sistemų (toliau – informacinės sistemos) elektroninės informacijos saugos politiką ir kibernetinio saugumo politiką (toliau – elektroninės informacijos saugos politika).

2. Saugos nuostatai taikomi tvarkant informacines sistemas, nurodytas Inspekcijos valdomų valstybės ir kitų informacinių sistemų sąraše (priedas).

3. Saugos nuostatai įgyvendinami pagal Inspekcijos viršininko tvirtinamus informacinių sistemų elektroninės informacijos saugos politiką įgyvendinančius dokumentus: saugaus elektroninės informacijos tvarkymo taisykles, naudotojų administravimo taisykles, veiklos tęstinumo valdymo planą (toliau – saugos politiką įgyvendinantys dokumentai).

4. 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), vartojamas sąvokas.

5. Informacinių sistemų elektroninės informacijos sauga ir kibernetinis saugumas – tai elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas.

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

6.1. sudaryti sąlygas saugiai tvarkyti elektroninę informaciją;

6.2. užtikrinti, kad elektroninė informacija būtų patikima ir apsaugota nuo atsitiktinio ar

neteisėto sunaikinimo, pakeitimo, atskleidimo, praradimo, taip pat nuo bet kokio kito neteisėto tvarkymo;

6.3. vykdyti elektroninės informacijos saugos ir kibernetinių incidentų (toliau – saugos incidentai) prevenciją.

7. Informacinių sistemų elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

7.1. elektroninės informacijos tvarkymo bei jos naudojimo kontrolė;

7.2. elektroninės informacijos tvarkymui naudojamos techninės ir programinės įrangos kontrolė;

7.3. informacinėse sistemose tvarkomų asmens duomenų apsauga;

7.4. informacinių sistemų veikos tęstinumo užtikrinimas.

8. Informacinių sistemų elektroninės informacijos saugai užtikrinti kompleksiškai naudojamos organizacinės, techninės ir programinės priemonės.

9. Saugos nuostatų reikalavimai taikomi:

9.1. informacinių sistemų valdytojui ir tvarkytojui – Inspekcijai, A. Vienuolio g. 8, Vilnius;

9.2. informacinių sistemų tvarkytojams, nurodytiems informacinių sistemų nuostatuose;

9.3. Inspekcijos paskirtam saugos įgaliotiniui (toliau – saugos įgaliotinis);

9.4. Inspekcijos paskirtiems administratoriams (toliau – administratorius);

9.5. informacinių sistemų naudotojams;

9.6. paslaugų, susijusių su informacinėmis sistemomis, teikėjams (toliau – paslaugų teikėjas).

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

11. 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.

12. Paslaugų teikėjai privalo įsipareigoti saugoti duomenų ir informacijos paslaptį bei pasirašyti su informacinių sistemų valdytoju suderintą asmens duomenų tvarkymo sutartį. Įsipareigojimas saugoti duomenų ir informacijos paslaptį galioja ir pasibaigus paslaugų teikimo laikui ar nutraukus šią veiklą.

13. Informacinių sistemų valdytoja atlieka informacinių sistemų nuostatuose nustatytas funkcijas, o taip pat:

13.1. tvirtina Saugos nuostatus, saugos politiką įgyvendinančius dokumentus, kitus dokumentus, susijusius su elektroninės informacijos sauga;

13.2. prižiūri ir kontroliuoja, kad informacinės sistemos būtų tvarkomos vadovaujantis informacinių sistemų nuostatais, Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais;

13.3. priima sprendimus dėl techninių ir programinių priemonių, būtinų elektroninės informacijos saugai užtikrinti, įsigijimo, įdiegimo ir modernizavimo;

13.4. rengia ir tvirtina informacinių technologijų saugos atitikties vertinimo metu nustatytų trūkumų šalinimo planą;

13.5. koordinuoja informacinių sistemų tvarkytojų darbą įgyvendinant elektroninės informacijos saugos reikalavimus;

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

13.7. priima sprendimus dėl informacinių sistemų elektroninės informacijos saugos priemonių finansavimo;

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

13.9. užtikrina saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

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

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

13.12. užtikrina, kad informacinės sistemos veiktų nepertraukiamai;

13.13. skiria saugos įgaliotinį ir administratorių;

13.14. skiria arba Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatyta tvarka parenka techninį administratorių;

13.15. vykdo kibernetinio saugumo organizavimo ir užtikrinimo funkcijas, nustatytas Kibernetinio saugumo įstatyme, 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), ir kituose kibernetinį saugumą reglamentuojančiuose teisės aktuose;

13.16. registruoja ir valdo saugos incidentus;

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

14. Informacinių sistemų tvarkytojai, nurodyti informacinių sistemų nuostatuose, atlieka šias funkcijas:

14.1. užtikrina tinkamą informacinių sistemų valdytojos priimtų teisės aktų ir rekomendacijų, susijusių su elektroninės informacijos sauga, įgyvendinimą;

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

14.3. pagal kompetenciją valdo informacinių sistemų kompiuterinių darbo vietų saugos incidentus, informuoja apie juos saugos įgaliotinį ir kitas atsakingas institucijas, šalina šiuos incidentus;

14.4. teikia pasiūlymus informacinių sistemų valdytojai dėl informacinių sistemų saugos tobulinimo;

14.5. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose, Saugos nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

15. Informacinių sistemų tvarkytojai užtikrina tvarkytojo įstaigoje tvarkomos elektroninės informacijos saugą. Informacinių sistemų tvarkytojų vadovai atsako už reikiamų organizacinių ir techninių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos nuostatuose ir informacinių sistemų saugos politiką įgyvendinančiuose dokumentuose nustatyta tvarka.

16. Saugos įgaliotinis:

16.1. supažindina administratorius ir informacinės sistemos naudotojus su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, atsakomybe už Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų nuostatų pažeidimus;

16.2. rengia Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų projektus;

16.3. koordinuoja ir prižiūri informacinių sistemų elektroninės informacijos saugos politikos įgyvendinimą;

16.4. koordinuoja saugos incidentų tyrimą;

16.5. teikia pasiūlymus Inspekcijos viršininkui dėl:

16.5.1. informacinių sistemų informacinių technologijų saugos atitikties vertinimo atlikimo;

16.5.2. administratoriaus paskyrimo;

16.5.3. Saugos nuostatų ir saugos politiką įgyvendinančių dokumentų priėmimo, keitimo ar panaikinimo;

16.6. teikia administratoriui, prireikus ir kitiems informacinių sistemų valdytojo ir tvarkytojų darbuotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės

informacijos saugos politikos įgyvendinimu;

16.7. pagal kompetenciją dalyvauja atliekant informacinių sistemų informacinių technologijų atitikties saugos reikalavimams vertinimą bei informacinių sistemų rizikos vertinimą;

16.8. ne rečiau kaip kartą per kalendorinius metus organizuoja administratorių ir informacinių sistemų naudotojų saugos mokymus (surengdamas saugos tematikos mokymus, pateikdamas mokymų medžiagą Inspekcijos interneto svetainėje arba organizuodamas mokymo paslaugų įsigijimą ar kitais būdais), reguliariai įvairiais būdais informuoja informacinių sistemų naudotojus apie elektroninės informacijos saugos problemas, teikia konsultacijas ir rekomendacijas (elektroniniu paštu, telefonu ir pan.);

16.9. dalyvauja tiriant saugos incidentus;

16.10. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, informacinių sistemų nuostatuose, Saugos nuostatuose bei saugos politiką įgyvendinančiuose dokumentuose nustatytas funkcijas.

17. Saugos įgaliotinis negali atlikti administratorių funkcijų.

18. Administratoriai atlieka funkcijas, susijusias su informacinių sistemų naudotojų administravimu, informacinės sistemos komponentais (kompiuteriais, operacinėmis sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, elektroninės informacijos perdavimu tinklais, bylų serveriais ir kitais), šių informacinių sistemų komponentų sąranka, informacinių sistemų pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena, reagavimu į saugos incidentus ir jų valdymu, taip pat privalo vykdyti visus saugos įgaliotinio nurodymus ir pavedimus, susijusius su informacinės sistemos saugos užtikrinimu, ir nuolat teikti saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę.

19. Inspekcijos skiriami administratoriai:

19.1. pagrindinis administratorius, kuris prižiūri informacinių sistemų infrastruktūrą, užtikrina jos veikimą ir informacinių sistemų elektroninės informacijos saugą:

19.1.1 pagal kompetenciją reaguoja į saugos incidentus ir juos valdo, atlieka įsilaužimų į informacines sistemas aptikimo funkcijas;

19.1.2 dalyvauja atliekant informacinių sistemų rizikos vertinimą ir informacinių sistemų informacinių technologijų atitikties saugos reikalavimas vertinimą;

19.2. informacinių sistemų naudotojų administratorius, kuris atlieka informacinių sistemų naudotojų administravimo funkcijas (informacinių sistemų naudotojų registravimas ir išregistravimas, prieigos teisių suteikimas ir panaikinimas, informacinių sistemų naudotojų duomenų tvarkymas, klasifikatorių tvarkymas, registracijos žurnalų įrašų analizė ir kt.);

19.3. informacinių sistemų infrastruktūros palaikymo administratoriai, kurie atlieka

funkcijas, susijusias su informacinių sistemų komponentais, šių informacinių sistemų komponentų sąranka:

19.3.1. kompiuterių tinklų administratorius atlieka šias funkcijas:

19.3.1.1. užtikrina kompiuterių tinklų veikimą;

19.3.1.2. projektuoja kompiuterių tinklus;

19.3.1.3. diegia, konfigūruoja ir prižiūri kompiuterių tinklų aktyviąją įrangą;

19.3.1.4. administruoja ugniasienes;

19.3.1.5. administruoja maršrutizatorius ir komutatorius;

19.3.1.6. administruoja pagalbinę įrangą (UPS, fizines linijas ir pan.);

19.3.1.7. užtikrina kompiuterių tinklų saugumą (nustato pažeidžiamas vietas);

19.3.2. tarnybinių stočių administratorius atlieka šias funkcijas:

19.3.2.1. užtikrina tarnybinių stočių veikimą;

19.3.2.2. konfigūruoja tarnybinių stočių tinklo prieigą;

19.3.2.3. administruoja tarnybinių stočių naudotojų registracijos į tarnybines stotis duomenis;

19.3.2.4. stebi ir analizuoja tarnybinių stočių veiklą;

19.3.2.5. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;

19.3.2.6. diegia tarnybinių stočių programinės įrangos atnaujinimus, laikydamasis tos informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse nustatytos programinės įrangos keitimo ir atnaujinimo tvarkos;

19.3.2.7. užtikrina tarnybinių stočių saugą;

19.3.3. kitų informacinių sistemų infrastruktūros palaikymo administratoriai atlieka funkcijas, susijusias su kitų 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.

20. Administratoriai pagal kompetenciją yra atsakingi už tinkamą Saugos nuostatuose ir informacinių sistemų saugos politiką įgyvendinančiuose dokumentuose nustatytų funkcijų vykdymą.

21. Teisės aktai, kuriais vadovaujantis tvarkoma informacinių sistemų elektroninė informacija ir užtikrinama jos sauga:

21.1. 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 ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1);

21.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

21.3. Lietuvos Respublikos kibernetinio saugumo įstatymas;

21.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

21.5. Bendrųjų saugos reikalavimų aprašas;

21.6. Kibernetinio saugumo reikalavimų aprašas;

21.7. Techniniai valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimai, patvirtinti Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“ (toliau – Techniniai reikalavimai);

21.8. Informacinių sistemų nuostatai;

21.9. Lietuvos standartai LST EN ISO/IEC 27002 ir LST EN ISO/IEC 27001 bei Lietuvos ir tarptautiniai „Informacijos technologijos. Saugumo metodai“ grupės standartai, reglamentuojantys saugų duomenų tvarkymą;

21.10. kiti teisės aktai, reglamentuojantys elektroninės informacijos tvarkymo teisėtumą ir elektroninės informacijos saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

22. Informacinėse sistemose tvarkomos elektroninės informacijos svarbos kategorija, informacinių sistemų kategorijos bei priskyrimo tam tikrai kategorijai kriterijai nurodyti Inspekcijos valdomų valstybės ir kitų informacinių sistemų sąraše (priedas).

23. Informacinių sistemų asmens duomenų tvarkymas automatiniu būdu priskiriamas pirmajam saugumo lygiui, vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms 11.1 papunkčio nuostatomis.

24. Informacinių sistemų saugos priemonės parenkamos įvertinus galimus rizikos veiksnius elektroninės informacijos vientisumui, konfidencialumui ir prieinamumui.

25. Pagrindinės informacinių sistemų rizikos mažinimo priemonės išdėstomos rizikos įvertinimo ataskaitoje, kurią kasmet ne vėliau nei iki spalio 1 dienos, o prireikus (pvz., įvykus esminiams organizaciniams, technologiniams ar kitiems informacinės sistemos pokyčiams) ir neeilinio rizikos įvertinimo ataskaitą iki informacinių sistemų valdytojos nurodytos datos, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės

standartus, rengia saugos įgaliotinis, įvertinęs galinčius turėti įtakos elektroninės informacijos saugai rizikos veiksnius, iš kurių svarbiausieji yra šie:

25.1. subjektyvūs netyčiniai (elektroninės informacijos tvarkymo klaidos ir apsirikimai, elektroninės informacijos ištrynimas, klaidingas elektroninės informacijos teikimas, fiziniai elektroninės informacijos technologijų sutrikimai, duomenų perdavimo tinklais sutrikimai, programinės įrangos klaidos, neteisingas veikimas ir kita);

25.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis informacine sistema elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugos pažeidimai, vagystės ir kita);

25.3. veiksniai, nurodyti Atleidimo nuo atsakomybės esant nenugalimos jėgos (force majeure) aplinkybėms taisyklių, patvirtintų Lietuvos Respublikos Vyriausybės 1996 m. liepos 15 d. nutarimu Nr. 84 „Dėl Atleidimo nuo atsakomybės esant nenugalimos jėgos (*force majeure*) aplinkybėms taisyklių patvirtinimo“, 3 punkte.

26. Rizikos įvertinimo ataskaitą bei jos kopijas informacinių sistemų valdytoja ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – 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 (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka.

27. Informacinių sistemų rizikos veiksnių vertinimui naudojama ARSIS. Informacinių sistemų grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinės sistemos kibernetiniam saugumui, vertinimas atliekamas kartu su informacinės sistemos rizikos vertinimu. Informacinės sistemos rizikos vertinimo metu gali būti atliekamas pažeidžiamumų testavimas imituojant kibernetines atakas bei vykdant kibernetinių incidentų imitavimo pratybas.

28. Informacinių technologijų saugos atitikties vertinimas atliekamas vadovaujantis Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo”. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijos ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi būti pateiktos ARSIS.

29. Elektroninės informacijos saugos būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis informacinių sistemų elektroninės informacijos saugos priemonėmis, kurios pasirenkamos atsižvelgiant į informacinių sistemų valdytojos skiriamus išteklius,

vadovaujantis šiais principais:

29.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

29.2. elektroninės informacijos saugos priemonės diegimo kainos turi atitikti saugomos elektroninės informacijos vertę;

29.3. esant galimybei, turi būti įdiegtos prevencinės korekcinės elektroninės informacijos saugos priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

30. Programinės įrangos, skirtos informacines sistemas apsaugoti nuo kenksmingosios programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir pan.), naudojimo nuostatos ir jos atnaujinimo reikalavimai:

30.1. informacinių sistemų tarnybinėse stotyse ir kompiuterizuotose darbo vietose turi būti naudojamos centralizuotai valdomos kenksmingosios programinės įrangos aptikimo priemonės, nuolat ieškančios ir blokuojančios kenksmingąją programinę įrangą, kurios turi būti reguliariai atnaujinamos automatiniu būdu ne rečiau kaip kartą per 24 valandas;

30.2. programinės įrangos konfigūravimas turi būti apsaugotas slaptažodžiu.

31. Programinės įrangos, įdiegtos informacinių sistemų tarnybinėse stotyse ir kompiuterizuotose darbo vietose, naudojimo nuostatos:

31.1. informacinių sistemų darbui turi būti naudojama tik legali ir patikrinta programinė įranga, įtraukta į leistinos programinės įrangos sąrašą. Leistinos programinės įrangos sąrašą tvirtina Inspekcija. Kitas informacinių sistemų tvarkytojas gali patvirtinti leistinos programinės įrangos sąrašą savo ir jam pavaldžių institucijų kompiuterinėms darbo vietoms. Inspekcijos tvirtinamą leistinos programinės įrangos sąrašą turi parengti ir pagal poreikį peržiūrėti bei prireikus atnaujinti saugos įgaliotinis kartu su pagrindiniu administratoriumi.

31.2. programinė įranga atnaujinama laikantis gamintojo reikalavimų;

31.3. programinės įrangos diegimą, šalinimą ir konfigūravimą atlieka administratoriai;

32. Informacinėse sistemose turi būti naudojamos tik tarnybinės išorinės duomenų laikmenos (USB, CD/DVD ir kt.) bei kiti tarnybiniai įrenginiai, kurie yra išduoti tarnybinėms funkcijoms vykdyti.

33. Informacinių sistemų programinis kodas privalo būti apsaugotas nuo atskleidimo neturintiems teisės su juo susipažinti asmenims.

34. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, įgaliotųjų serverių (angl. *proxy*) ir kt.) pagrindinės naudojimo nuostatos:

34.1. kompiuterių tinklai nuo viešųjų telekomunikacijų tinklų (interneto) turi būti atskirti ugniasienėmis, DOS ir DDOS atakų prevencijai skirta įranga bei įsilaužimų aptikimo ir prevencijos

įranga;

34.2. visas duomenų srautas į internetą ir iš jo turi būti filtruojamas naudojant apsaugą nuo virusų ir kitos kenksmingosios programinės įrangos;

34.3. turi būti naudojamos turinio filtravimo sistemos.

35. Informacinėse sistemose naudojamų interneto svetainių (toliau – svetainės) saugos valdymo reikalavimai:

35.1. svetainės turi atitikti Kibernetinio saugumo reikalavimų apraše ir Techniniuose reikalavimuose nustatytus reikalavimus;

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

35.3. informacinėse sistemose naudojamų svetainių sauga turi būti vertinama informacinių sistemų rizikos įvertinimo metu ir (arba) informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu.

36. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

36.1. tiesioginė prieiga prie informacinių sistemų elektroninės informacijos suteikiama įgyvendinus informacinių sistemų naudotojų autentifikavimo priemones – šie naudotojai savo tapatybę patvirtina slaptažodžiu ar kita autentifikavimo priemone; tiesioginė prieiga prie informacinių sistemų užtikrinama automatiniu būdu ištisą parą darbo ir poilsio dienomis;

36.2. prieiga prie informacinių sistemų suteikiama tik registruotiems informacinių sistemų naudotojams;

36.3. informacinių sistemų elektroninė informacija perduodama automatiniu būdu naudojant TCP/IP, HTTPS protokolus realiame laike (*angl. „On-line“* režimu) arba pagal informacinių sistemų duomenų teikimo sutartis, kuriose nustatytos perduodamos elektroninės informacijos specifikacijos ir kitos elektroninės informacijos perdavimo sąlygos bei tvarka.

37. Informacinių sistemų elektroninės informacijos perdavimui naudojamas Aplinkos ministerijos tinklas ir kiti saugūs elektroninių ryšių tinklai.

38. Informacinių sistemų naudotojų tarnybinėms funkcijoms vykdyti naudojamuose nešiojamuose kompiuteriuose turi būti naudojamas kompiuterio įjungimo slaptažodis.

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

39.1. informacinių sistemų elektroninės informacijos kopijos turi būti daromos automatiškai kiekvieną dieną; prireikus jas atkurti turi teisę atsakingas informacinių sistemų administratorius, kurio funkcijos aprašytos naudotojų administravimo taisyklėse ir kituose teisės aktuose,

reglamentuojančiuose IS darbą;

39.2. atkūrimas iš elektroninės informacijos kopijų privalo būti išbandomas.

40. Turi būti užtikrintas saugos incidentų, įvykusių informacinėse sistemose, registravimas, valdymas ir tyrimas Kibernetinių saugumo reikalavimų aprašo bei informacinių sistemų veiklos tęstinumo valdymo plano nustatyta tvarka:

40.1. registruojami informacinėse sistemose įvykę saugos incidentai ir nedelsiant į juos reaguojama, techninėmis ir programinėmis priemonėmis saugos incidentai valdomi, tiriami ir šalinami bei atkuriama sistemų veikla;

40.2. Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos ir kitoms atsakingoms institucijoms pagal kompetenciją pranešama apie įvykusius saugos incidentus, jų vertinimą ir suvaldymą.

41. Ne rečiau kaip kartą per mėnesį turi būti atliekama ugniasienių užfiksuotų įvykių analizė ir pastebėtos neatitiktys saugumo reikalavimams nedelsiant šalinamos.

42. Ne rečiau kaip kartą per mėnesį turi būti įvertinami kibernetiniam saugumui užtikrinti naudojamų priemonių programiniai atnaujinimai, klaidų taisymai ir šie atnaujinimai diegiami.

43. Perkant paslaugas, darbus ar įrangą, susijusius su informacinėmis sistemomis, jų projektavimu, kūrimu, diegimu, modernizavimu, priežiūra, palaikymu, saugos užtikrinimu, auditavimu, patalpų priežiūra, elektroninės informacijos perdavimo tinklais, taip pat kitus, suteikiančius teisę ir galimybę prieiti prie elektroninės informacijos, ją apdoroti, saugoti, keistis elektronine informacija ar tiekti informacinių technologijų infrastruktūros komponentus, pirkimo dokumentuose iš anksto turi būti nustatyta, kad paslaugų teikėjas, darbų vykdytojas ar techninės ir programinės įrangos tiekėjas – paslaugų teikėjas, privalo laikytis informacinių sistemų saugos dokumentuose nustatytų reikalavimų ir užtikrinti teikiamų paslaugų, vykdomų darbų ar tiekiamos įrangos atitiktį nustatytiems elektroninės informacijos saugos reikalavimams.

44. Į paslaugų pirkimo sutartyje turi būti numatyta nuostata, įpareigojanti paslaugų teikėją, jo darbuotojus, subteikėjus neatskleisti tretiesiems asmenims jokios informacijos, gautos vykdant šią sutartį, išskyrus tiek, kiek būtina sutarties vykdymui, o 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, nebent raštu patvirtinama, kad tam tikra pateikta informacija nėra konfidenciali.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

45. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu,

kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą, privalo tobulinti kvalifikaciją elektroninės informacijos saugos srityje.

46. Saugos įgaliotiniu, administratoriumi 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 jos paskyrimo praėję mažiau kaip vieneri metai.

47. 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, 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 (*Windows, Unix*) administravimo ir priežiūros patirties.

48. Administratoriai ir informacinių sistemų naudotojai turi būti susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais, pagal kompetenciją ir kitais teisės aktais bei standartais, reglamentuojančiais elektroninės informacijos saugą.

49. 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.

50. Informacinių sistemų naudotojai, atliekantys tarnybines funkcijas, susijusias su asmens duomenų tvarkymu bei teikimu, pasirašytinai supažindinami su asmens duomenų tvarkymą ir apsaugą reglamentuojančiais teisės aktais ir atsakomybe už jų pažeidimą bei raštu įpareigojami saugoti asmens duomenų paslaptį. Asmens duomenų paslaptį jie privalo saugoti ir pasibaigus darbo (tarnybos) santykiams, per visą asmens duomenų teisinės apsaugos laiką, jeigu Asmens duomenų teisinės apsaugos įstatymas nenumato ko kita.

51. Informacinių sistemų naudotojai, pastebėję saugos politiką įgyvendinančiuose dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai atitinkamos informacinės sistemos administratoriui ar saugos įgaliotiniui.

52. Informacinių sistemų naudotojai privalo:

52.1. turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti saugiai tvarkyti elektroninę informaciją;

52.2. nuolat kelti kvalifikaciją saugaus elektroninės informacijos tvarkymo kursuose, mokymuose, seminaruose;

52.3. įtarę, kad prisijungimo prie informacinės sistemos slaptažodis galėjo būti atskleistas kitam asmeniui, praradę ar kitaip netekę slaptažodžio, nedelsiant informuoti informacinės sistemos administratorių; nurodytais atvejais slaptažodis turi būti pakeistas Naudotojų administravimo taisyklių, patvirtintų Inspekcijos viršininko, nustatyta tvarka.

53. Informacinių sistemų naudotojams draudžiama:

53.1. atskleisti informacinės sistemos duomenis ar suteikti kitokią galimybę bet kokia forma su jais susipažinti tokios teisės neturintiems asmenims;

53.2. savavališkai diegti informacinės sistemos taikomosios programinės įrangos pakeitimus ir naujas versijas neturint tam suteiktos teisės;

53.3. atskleisti kitiems asmenims prisijungimo prie informacinės sistemos vardą, slaptažodį ar kitaip sudaryti sąlygas jais pasinaudoti;

53.4. naudoti informacinės sistemos duomenis kitokiais nei jų nuostatuose nurodytais tikslais bei savo pareigybės aprašyme nustatytų funkcijų vykdymo tikslais;

53.5. sudaryti sąlygas pasinaudoti informacinei sistemai tvarkyti naudojama technine ir programine įranga tokios teisės neturintiems asmenims (paliekant darbo vietą būtina užrakinti darbalaukį arba išjungti darbo stotį);

53.6. atlikti veiksmus, dėl kurių gali būti neteisėtai pakeisti, sunaikinti ar atskleisti informacinės sistemos duomenys, taip pat neatlikti būtinų veiksmų, kurie apsaugo informacinės sistemos duomenis;

53.7. atlikti bet kokius kitus neteisėtus informacinės sistemos tvarkymo veiksmus.

54. 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 mokymai organizuojami periodiškai, mokymus organizuoja saugos įgaliotinis.

V SKYRIUS
INFORMACINIŲ SISTEMŲ NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

55. Tvarkyti informacinių sistemų elektroninę informaciją gali tik informacinių sistemų naudotojai, susipažinę su Saugos nuostatais, saugos politiką įgyvendinančiais dokumentais ir kitais teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugą, taip pat

atsakomybe už saugos dokumentų nuostatų pažeidimus, ir sutikę laikytis saugos dokumentuose nustatytų reikalavimų. Pakartotinis supažindinimas yra vykdomas pasikeitus minėtiems dokumentams ir teisės aktams.

56. Informacinių sistemų naudotojų supažindinimą su Saugos nuostatais ir informacinių sistemų saugos politiką įgyvendinančiais dokumentais pagal kompetenciją organizuoja saugos įgaliotiniai.

57. Informacinių sistemų naudotojai su Saugos nuostatais ir informacinių sistemų saugos politiką įgyvendinančiais dokumentais bei atsakomybe už jų reikalavimų nesilaikymą supažindinami pasirašytinai arba elektroniniu būdu, užtikrinančiu supažindinimo įrodomumą (jungiantis prie informacinės sistemos per naudotojo sąsają ar pan.).

58. Informacinių sistemų naudotojai, pažeidę Saugos nuostatų ir informacinių sistemų saugos politiką įgyvendinančių dokumentų nuostatas, atsako teisės aktų nustatyta tvarka.

59. Saugos nuostatai ir informacinių sistemų saugos politiką įgyvendinantys dokumentai turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Saugos nuostatai ir informacinių sistemų saugos politiką įgyvendinantys dokumentai turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams. Saugos įgaliotiniai pagal kompetenciją atsakingi, kad informacinių sistemų naudotojai būtų informuoti apie jų pakeitimą ir (ar) pripažinimą netekusiais galios.

_____

Kai kurių Valstybinės teritorijų planavimo ir statybos inspekcijos valdomų valstybės ir kitų informacinių sistemų duomenų saugos nuostatų
priedas

VALSTYBINĖS TERITORIJŲ PLANAVIMO IR STATYBOS INSPEKCIJOS PRIE APLINKOS MINISTERIJOS VALDOMŲ VALSTYBĖS IR KITŲ INFORMACINIŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	Informacinės sistemos pavadinimas	Informacinės sistemos elektroninės informacijos svarbos kategorija	Informacinės sistemos kategorija	Informacinės sistemos priskyrimo kategorijai kriterijai*
1.	Lietuvos Respublikos teritorijų planavimo dokumentų rengimo ir teritorijų planavimo proceso valstybinės priežiūros informacinė sistema	svarbi	antra	8.1, 8.3 ir 12.2 papunkčiai
2.	Lietuvos Respublikos statybos leidimų ir statybos valstybinės priežiūros informacinė sistema „Infostatyba“	svarbi	antra	8.1, 8.3 ir 12.2 papunkčiai
3.	Dokumentų ir procesų valdymo sistema „Avilys“	vidutinės svarbos	trečia	9.1, 9.2 ir 12.3 papunkčiai

* 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“.

_____