Suvestinė redakcija nuo 2021-01-20

Įsakymas paskelbtas: TAR 2019-02-27, i. k. 2019-03276

LIETUVOS RESPUBLIKOS
RYŠIŲ REGULIAVIMO TARNYBOS
DIREKTORIUS

ĮSAKYMAS
DĖL LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS INFORMACINIŲ SISTEMŲ SAUGOS DOKUMENTŲ PATVIRTINIMO

2019 m. vasario 26 d. Nr. 1V-240
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, 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, 8 ir 12 punktais ir 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:

1.1. Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų saugos nuostatus;

1.2. Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles;

1.3. Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų veiklos tęstinumo valdymo planą;

1.4. Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų naudotojų administravimo taisykles.

2. S k i r i u:

2.1. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus vyriausiąjį patarėją Sigitą Jurkevičių Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų saugos įgaliotiniu;

2.2. Lietuvos Respublikos ryšių reguliavimo tarnybos Administracinio departamento Informacinių technologijų skyriaus patarėją Laimį Tamošiūną Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų administratoriumi.

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

3.1. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2011 m. gruodžio 14 d. įsakymą Nr. 1V-1287 „Dėl Radijo dažnių spektro valdymo informacinės sistemos saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais;

3.2. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2012 m. balandžio 13 d. įsakymą Nr. 1V-476 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos saugaus elektroninės informacijos tvarkymo taisyklių, informacinės sistemos naudotojų administravimo taisyklių ir informacinės sistemos veiklos tęstinumo valdymo plano patvirtinimo“;

3.3. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2016 m. rugsėjo 26 d. įsakymą Nr. 1V-1006 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais;

3.4. Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2017 m. gruodžio 22 d. įsakymą Nr. 1V-1291 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos saugos politiką įgyvendinančių dokumentų patvirtinimo“.

4. N u r o d a u paskelbti šį įsakymą Teisės aktų registre.

Tinklų reguliavimo departamento direktorius,
pavaduojantis direktorių Viktoras Syrusas

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2019 m. vasario 4 d. raštu Nr. (4.2 E) 6K-83

PATVIRTINTA
Lietuvos Respublikos ryšių reguliavimo
tarnybos direktoriaus 2019 m. vasario 26 d.
įsakymu Nr. 1V-240

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS INFORMACINIŲ SISTEMŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – Tarnyba) informacinių sistemų (toliau – IS) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Saugos nuostatų reikalavimai taikomi valstybės IS, nurodytoms Saugos nuostatų priede pateiktame Tarnybos valstybės IS sąraše, ir Tarnybos vidaus administravimui skirtoms IS.

3. Tarnybos elektroninės informacijos saugos ir kibernetinio saugumo politika įgyvendinama pagal Saugos nuostatus ir Tarnybos direktoriaus tvirtinamus Tarnybos IS saugos politikos įgyvendinamuosius dokumentus: Tarnybos IS saugaus elektroninės informacijos tvarkymo taisykles, Tarnybos IS naudotojų administravimo taisykles, Tarnybos IS veiklos tęstinumo valdymo planą (toliau kartu – Saugos dokumentai).

4. Saugos nuostatuose vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo 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 elektroninės informacijos saugos reikalavimų aprašas) ir Lietuvos standartuose LST ISO 27000.

5. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

5.1. sudaryti sąlygas saugiai automatizuotu 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.

6. Elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti naudojamos organizacinės, techninės, programinės ir fizinės elektroninės informacijos apsaugos priemonės.

7. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetinės kryptys:

7.1. elektroninės informacijos konfidencialumo užtikrinimas;

7.2. elektroninės informacijos vientisumo užtikrinimas;

7.3. elektroninės informacijos prieinamumo užtikrinimas;

7.4. asmens duomenų apsauga;

7.5. IS veiklos tęstinumo užtikrinimas;

7.6. prieigos prie IS kontrolė;

7.7. rizikos valdymas;

7.8. IS naudotojų mokymas elektroninės informacijos saugos ir kibernetinio saugumo klausimais;

7.9. organizacinių, techninių, programinių, teisinių, informacijos sklaidos ir kitų priemonių, skirtų elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė.

8. Saugos nuostatai taikomi:

8.1. IS valdytojui ir tvarkytojui – Tarnybai, kurios adresas Mortos g. 14, Vilnius;

8.2. IS saugos įgaliotiniui;

8.3. IS administratoriui;

8.4. IS naudotojams.

9. Tarnybos, kaip IS tvarkytojos ir valdytojos, funkcijos:

9.1. atlieka elektroninės informacijos tvarkymo ir elektroninės informacijos saugos reikalavimų bei 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 reikalavimai) nustatytų reikalavimų laikymosi priežiūrą ir kontrolę;

9.2. nagrinėja pasiūlymus dėl IS veiklos, elektroninės informacijos saugos ir kibernetinio saugumo, juos apibendrina ir priima sprendimus dėl IS tobulinimo;

9.3. priima sprendimus dėl techninių ir programinių priemonių, būtinų elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įsigijimo, diegimo ir modernizavimo;

9.4. skiria IS saugos įgaliotinį ir IS administratorių;

9.5. rengia ir priima teisės aktus, užtikrinančius duomenų tvarkymo teisėtumą ir elektroninės informacijos saugą ir kibernetinį saugumą, atlieka šių teisės aktų nuostatų laikymosi priežiūrą;

9.6. užtikrina elektroninės informacijos saugą, kibernetinį saugumą ir saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais (automatiniu būdu);

9.7. tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, priima sprendimus dėl rizikos vertinimo rezultatų;

9.8. tvirtina informacinių technologijų saugos atitikties vertinimo metu pastebėtų trūkumų šalinimo planą;

9.9. atlieka kitas Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, IS nuostatuose bei Saugos dokumentuose nustatytas funkcijas.

10. IS saugos įgaliotinio funkcijos:

10.1. teikia Tarnybos direktoriui pasiūlymus dėl Tarnybos informacinių technologijų saugos atitikties vertinimo atlikimo, Saugos dokumentų priėmimo, keitimo ir panaikinimo;

10.2. koordinuoja elektroninės informacijos saugos ir kibernetinio saugumo incidentų tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis šiuos incidentus, neteisėtas veikas, susijusias su šiais incidentais;

10.3. teikia IS administratoriui, IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos ir kibernetinio saugumo įgyvendinimu;

10.4. organizuoja IS naudotojų supažindinimą su Saugos dokumentais;

10.5. koordinuoja Saugos dokumentų reikalavimų vykdymą;

10.6. organizuoja IS rizikos ir informacinių technologijų saugos atitikties vertinimą;

10.7. organizuoja IS naudotojams mokymus elektroninės informacijos saugos klausimais;

10.8. atlieka kitas Saugos nuostatuose, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą, IS saugos įgaliotiniui nustatytas funkcijas.

11. IS saugos įgaliotinis negali atlikti IS administratoriaus funkcijų.

12. IS administratorius atlieka šias funkcijas:

12.1. užtikrina kompiuterinių tinklų veikimą;

12.2. projektuoja kompiuterinius tinklus;

12.3. atlieka IS naudotojų teisių valdymo funkcijas (IS naudotojų duomenų administravimą, klasifikatorių tvarkymą, IS naudotojų veiksmų, registracijos žurnalų įrašų analizę ir kita);

12.4. diegia, konfigūruoja ir prižiūri kompiuterinių tinklų aktyviąją įrangą;

12.5. užtikrina kompiuterinių tinklų saugumą (nustato pažeidžiamas vietas);

12.6. pagal kompetenciją reaguoja į elektroninės informacijos saugos ir kibernetinio saugumo incidentus ir juos valdo, atlieka įsilaužimų į IS aptikimo funkcijas;

12.7. administruoja ugniasienes, maršrutizatorius, komutatorius ir pagalbinę įrangą (nepertraukiamo maitinimo šaltinius, fizines linijas ir panašiai);

12.8. užtikrina tarnybinių stočių veikimą;
12.9. konfigūruoja tarnybinių stočių tinklo prieigą;
12.10. stebi ir analizuoja tarnybinių stočių veiklą;
12.11. diegia ir konfigūruoja tarnybinių stočių programinę įrangą;
12.12. diegia tarnybinių stočių programinės įrangos atnaujinimus;
12.13. užtikrina tarnybinių stočių saugą;
12.14. užtikrina duomenų bazių veikimą;
12.15. tvarko duomenų bazių programinę įrangą;
12.16. diegia duomenų bazių programinės įrangos atnaujinimus;
12.17. kuria ir atkuria atsargines elektroninės informacijos kopijas;
12.18. stebi duomenų bazes ir optimizuoja jų funkcionavimą;
12.19. ne rečiau kaip kartą per metus ir (arba) po IS pokyčio tikrina (peržiūri) IS sąranką ir IS būsenos rodiklius;
12.20. vykdo visus IS saugos įgaliotinio nurodymus ir pavedimus dėl elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo, nuolat teikia IS saugos įgaliotiniui informaciją apie saugą užtikrinančių pagrindinių komponentų būklę;
12.21. atlieka IS pažeidžiamų vietų nustatymo, saugumo reikalavimų atitikties nustatymo ir stebėsenos funkcijas;
12.22. atlieka kitas Saugos nuostatuose ir Saugos dokumentuose nustatytas funkcijas.
13. Atlikdamas IS sąrankos pakeitimus, IS administratorius turi laikytis IS pokyčių valdymo tvarkos, nustatytos Tarnybos IS saugaus elektroninės informacijos tvarkymo taisyklėse.
14. Teisės aktai, kuriais vadovaujamasi tvarkant elektroninę informaciją ir užtikrinant jos saugą:
14.1. Lietuvos Respublikos kibernetinio saugumo įstatymas;
14.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;
14.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;
14.4. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;
14.5. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašas, patvirtintas 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 saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – Techniniai elektroninės informacijos saugos reikalavimai);
Papunkčio pakeitimai:
Nr. (1.9E)1V-51, 2021-01-13, paskelbta TAR 2021-01-19, i. k. 2021-00851

14.6. Kibernetinio saugumo reikalavimai;
14.7. 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);
14.8. kiti teisės aktai, reglamentuojantys elektroninės informacijos tvarkymą, elektroninės informacijos saugą ir kibernetinį saugumą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

15. Elektroninės informacijos svarbos kategorija, IS kategorijos ir priskyrimo prie tam tikros kategorijos kriterijai nurodyti Saugos nuostatų priede.
16. IS saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos ir tarptautinius „Informacijos technologija. Saugumo technika“ grupės

standartus, kasmet organizuoja IS rizikos vertinimą, kuris atliekamas vertinant rizikos veiksnius, galinčius turėti įtakos elektroninės informacijos saugai ir kibernetiniam saugumui, jų galimą žalą, pasireiškimo tikimybę ir pobūdį, galimus rizikos valdymo būdus, rizikos priimtinumo kriterijus. Svarbiausi rizikos veiksniai:

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

16.2. subjektyvūs tyčiniai (nesankcionuotas IS naudojimas elektroninei informacijai gauti, elektroninės informacijos pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymas, saugos pažeidimai, vagystės ir kita);

16.3. 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.

17. IS rizikos įvertinimo rezultatai išdėstomi rizikos įvertinimo ataskaitoje, kuri teikiama Tarnybos direktoriui.

18. Atsižvelgdamas į rizikos įvertinimo ataskaitą, Tarnybos direktorius prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

19. Elektroninės informacijos saugos ir kibernetinio saugumo būklė gerinama techninėmis, programinėmis, organizacinėmis ir kitomis elektroninės informacijos saugos ir kibernetinio saugumo priemonėmis, kurios pasirenkamos atsižvelgiant į Tarnybos turimus išteklius, vadovaujantis šiais principais:

19.1. likutinė rizika turi būti sumažinta iki priimtino lygio;

19.2. elektroninės informacijos saugos ir kibernetinio saugumo priemonės diegimo kaina turi būti proporcinga saugomos elektroninės informacijos vertei;

19.3. atsižvelgiant į priemonių efektyvumą ir taikymo tikslingumą, turi būti įdiegtos prevencinės, detekcinės ir korekcinės elektroninės informacijos saugos ir kibernetinio saugumo priemonės.

20. Rizikos įvertinimo ataskaitos kopiją IS saugos įgaliotinis ne vėliau kaip per 5 darbo dienas nuo rizikos įvertinimo ataskaitos patvirtinimo pateikia Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai (toliau – ARSIS).

21. Siekiant užtikrinti Saugos dokumentuose nustatytų elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų įgyvendinimo kontrolę, IS saugos įgaliotinis organizuoja informacinių technologijų saugos atitikties vertinimą, kuris atliekamas Informacinių technologijų saugos atitikties vertinimo metodikoje, patvirtintoje Lietuvos Respublikos vidaus reikalų ministro 2004 m. gegužės 6 d. įsakymu Nr. 1V-156 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“, nustatyta tvarka.

22. Atlikus informacinių technologijų saugos atitikties įvertinimą, IS saugos įgaliotinis rengia ir teikia Tarnybos direktoriui informacinių technologijų saugos įvertinimo ataskaitą. Atsižvelgdamas į informacinių technologijų saugos atitikties įvertinimo ataskaitą, IS saugos įgaliotinis prireikus parengia pastebėtų trūkumų šalinimo planą, kurį tvirtina Tarnybos direktorius.

23. Informacinių technologijų saugos atitikties vertinimas turi būti organizuojamas ne rečiau kaip kartą per dvejus metus, jei teisės aktuose nenustatyta kitaip.

24. Informacinių technologijų saugos atitikties įvertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas IS saugos įgaliotinis ne vėliau kaip per 5 darbo dienas nuo šių dokumentų patvirtinimo pateikia ARSIS.

25. Atitikties Kibernetinio saugumo reikalavimuose nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas (toliau – kibernetinio saugumo vertinimas) turi būti organizuojamas ne rečiau kaip kartą per kalendorinius metus.

26. Kibernetinio saugumo vertinimo metu atliekamas kibernetinių atakų imitavimas, kuris atliekamas šiais etapais:

26.1. Planavimo etapas. IS saugos įgaliotinis parengia kibernetinių atakų imitavimo planą, kuriame apibrėžiami kibernetinių atakų imitavimo tikslai, aprašomi planuojamų imituoti kibernetinių atakų tipai (išorinės ir (ar) vidinės), kibernetinių atakų imitavimo būdai (juodosios dėžės (angl. *black box*), baltosios dėžės (angl. *white box*) ir (arba) pilkosios dėžės (angl. *grey box*)), galima neigiama įtaka IS veiklai, kibernetinių atakų imitavimo metodologija, programiniai ir (arba) techniniai įrankiai ir priemonės, planuojami testai, nurodomi už plano vykdymą atsakingi asmenys ir jų kontaktai. Kibernetinių atakų imitavimo planas vykdomas tik jį suderinus su Tarnybos direktoriumi.

26.2. Žvalgybos (angl. *reconnaissance*) ir aptikimo (angl. *discovery*) etapas. Surenkama informacija apie IS perimetrą, tinklo mazgus, tinklo mazguose veikiančių tarnybinių stočių ir kitų tinklo įrenginių operacines sistemas ir programinę įrangą, paslaugas (angl. *services*), pažeidžiamumą, konfigūracijas ir kitą sėkmingai kibernetinei atakai įvykdyti reikalingą informaciją.

26.3. Kibernetinių atakų imitavimo etapas. Atliekami kibernetinių atakų imitavimo plane numatyti testai.

26.4. Ataskaitos parengimo etapas. IS saugos įgaliotinis kibernetinių atakų imitavimo rezultatus išdėsto ataskaitoje, kurioje detalizuojami kibernetinių atakų imitavimo plane numatytų testų rezultatai, pateikiamas jų palyginimas su planuotais rezultatais, nurodomi visi aptikti pažeidžiamumai ir rekomendacijos jiems pašalinti. Kibernetinių atakų imitavimo rezultatai turi būti pagrįsti patikimais įrodymais ir rizikos įvertinimu. Jeigu nustatoma incidentų valdymo ir šalinimo, taip pat IS nepertraukiamos veiklos užtikrinimo trūkumų, turi būti tobulinamas Tarnybos IS veiklos tęstinumo planas.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

27. IS naudojamų svetainių saugos valdymo reikalavimai:

27.1. Svetainės turi atitikti Kibernetinio saugumo reikalavimuose ir Techniniuose elektroninės informacijos saugos reikalavimuose nustatytus reikalavimus.

27.2. Svetainių užkardos turi būti sukonfigūruotos taip, kad prie svetainių turinio valdymo sistemų būtų galima jungtis tik iš vidinio Tarnybos kompiuterinio tinklo arba nustatytų IP (angl. *Internet Protocol*) adresų.

27.3. Turi būti pakeistos numatytosios prisijungimo prie svetainių turinio valdymo sistemų ir administravimo skydų (angl. *panel*) nuorodos (angl. *default path*) ir slaptažodžiai.

27.4. Turi būti užtikrinama, kad prie svetainių turinio valdymo sistemų ir administravimo skydų būtų galima jungtis tik naudojantis šifruotu ryšiu.

27.5. Svetainių sauga turi būti vertinama IS rizikos vertinimo ir informacinių technologijų saugos atitikties vertinimo metu.

28. Programinės įrangos, skirtos apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir panašiai), naudojimo nuostatos ir atnaujinimo reikalavimai:

28.1. Tarnybinėse stotyse ir vidinių IS naudotojų kompiuteriuose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiu laiku priemonės.

28.2. Komponentai be kenksmingos programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu IS rizikos vertinimo metu patvirtinama, kad šių komponentų rizika yra priimtina.

28.3. Kenksmingos programinės įrangos aptikimo priemonės turi atsinaujinti automatiškai ne rečiau kaip kartą per 24 valandas.

28.4. IS administratorius turi būti automatiškai elektroniniu paštu informuojamas apie tai, kuriems IS posistemiams, funkciškai savarankiškoms sudedamosioms dalims, vidinių IS naudotojų

kompiuteriams ir kitiems komponentams yra pradelstas kenksmingos programinės įrangos aptikimo priemonių atsinaujinimo laikas, kenksmingos programinės įrangos aptikimo priemonės netinkamai funkcionuoja arba yra išjungtos.

29. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo nuostatos:

29.1. Tarnybinėse stotyse ir IS naudotojų kompiuteriuose turi būti naudojama tik teisėta programinė įranga.

29.2. Vidinių IS naudotojų kompiuteriuose naudojama programinė įranga turi būti įtraukta į leistinos naudoti programinės įrangos sąrašą, kurį rengia, ne rečiau kaip kartą per metus peržiūri ir prireikus atnaujina IS saugos įgaliotinis.

29.3. Tarnybinių stočių ir vidinių IS naudotojų kompiuterių operacinės sistemos, kibernetiniam saugumui užtikrinti naudojamų priemonių ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai, klaidų pataisymai turi būti operatyviai išbandomi ir įdiegiami.

29.4. IS administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumo svarbos lygius posistemiuose, funkciškai savarankiškose sudedamosiose dalyse, vidinių IS naudotojų kompiuteriuose ir apie tai informuoti IS saugos įgaliotinį.

29.5. Programinė įranga turi būti prižiūrima ir atnaujinama laikantis gamintojo reikalavimų ir rekomendacijų.

29.6. Programinės įrangos diegimą, konfigūravimą, priežiūrą ir gedimų šalinimą turi atlikti IS administratorius arba tokias paslaugas teikiantys paslaugų teikėjai.

29.7. Programinė įranga turi būti testuojama naudojant atskirą testavimo aplinką.

29.8. Programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą 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.

30. Kompiuterių tinklo filtravimo įrangos (užkardų, turinio kontrolės sistemų, tarnybinių stočių ir kitų) pagrindinės naudojimo nuostatos:

30.1. Kompiuterių tinklo ir užkardų konfigūracija peržiūrima ne rečiau kaip kartą per metus. Peržiūrą inicijuoja IS saugos įgaliotinis, o ją vykdo IS administratorius.

30.2. Kompiuterių tinklai turi būti atskirti nuo viešųjų elektroninių ryšių tinklų ir interneto naudojant užkardas, automatinę įsilaužimų aptikimo ir prevencijos įrangą, atkirtimo nuo paslaugos, dedikuoto atkirtimo nuo paslaugos įrangą.

30.3. Kompiuterių tinklų perimetro apsaugai turi būti naudojami filtrai, apsaugantys vidinių IS 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.

30.4. Apsaugai nuo elektroninės informacijos nutekinimo turi būti naudojama duomenų srautų analizės ir kontrolės įranga.

30.5. Turi būti naudojamos turinio filtravimo sistemos.

30.6. Turi būti naudojamos taikomųjų programų kontrolės sistemos.

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

31.1. Duomenys perduodami automatiškai TCP/IP protokolu realiuoju laiku arba asinchroniniu režimu tik pagal IS nuostatuose ir duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką.

31.2. Už duomenų teikimo ir gavimo sutartyse nurodomų saugos reikalavimų nustatymą, suformulavimą ir įgyvendinimo organizavimą atsakingas IS saugos įgaliotinis.

31.3. Duomenys perduodami šifruotais ryšio kanalais.

31.4. Duomenims registruoti naudojamas saugus hipertekstų persiuntimo protokolas (angl. *Hypertext Transfer Protocol Secure*, HTTPS).

31.5. Duomenims perduoti naudojamas saugaus valstybinio duomenų perdavimo tinklas (SVDPT).

31.6. Duomenims perduoti naudojamas virtualus privatus tinklas.

31.7. Šifro raktų ilgiai, šifro raktų generavimo algoritmai, šifro raktų apsikeitimo protokolai, elektroninio parašo šifravimo algoritmai ir kiti šifravimo algoritmai nustatomi atsižvelgiant į Lietuvos ir tarptautinių organizacijų ir standartų rekomendacijas, Kibernetinio saugumo reikalavimus.

31.8. Naudojamų šifravimo priemonių patikimumas vertinamas neeilinio arba kasmetinio rizikos vertinimo metu. Nustačius saugumo spragų šifravimo algoritmuose, šifravimo priemonės turi būti operatyviai keičiamos.

32. Pagrindiniai atsarginių duomenų kopijų darymo ir atkūrimo reikalavimai:

32.1. Atsarginės duomenų kopijos turi būti daromos periodiškai (visų duomenų kopija – kartą per savaitę) vadovaujantis Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninės informacijos atsarginio kopijavimo, atsarginių kopijų saugojimo ir atkūrimo iš atsarginių kopijų taisyklėmis, patvirtintomis Tarnybos direktoriaus 2018 m. gegužės 17 d. įsakymu Nr. 1V-477 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninės informacijos atsarginio kopijavimo, atsarginių kopijų saugojimo ir atkūrimo iš atsarginių kopijų taisyklių patvirtinimo“.

32.2. Atsarginių kopijų laikmenos turi būti pažymimos taip, kad jas būtų galima atpažinti.

32.3. Už atsarginių duomenų kopijų darymo ir atkūrimo, taikomosios programinės įrangos (aplikacijų) kopijų darymo inicijavimą atsakingas IS saugos įgaliotinis, o už vykdymą – IS administratorius.

32.4. Atsarginės duomenų kopijos turi būti saugomos užrakintoje nedegioje spintoje, kitose patalpose arba kitame pastate, nei yra įrašymo įrenginys.

33. Leistinos kompiuterių ir kitų mobiliųjų įrenginių naudojimo ribos:

33.1. IS duomenų tvarkymui leidžiama naudoti tik leistinus stacionariuosius ir nešiojamuosius kompiuterius, atitinkančius IS valdytojo nustatytus elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus.

33.2. Jeigu nešiojamasis kompiuteris naudojamas ne tik Tarnybos patalpose, turi būti įdiegtos papildomos saugos priemonės, taikytinos tokiems kompiuteriams (šifravimas, papildomas tapatybės patvirtinimas, prisijungimo ribojimai, rakinimo įrenginių naudojimas ir panašiai).

33.3. Nešiojamuosiuose kompiuteriuose neturi būti jokios svarbios informacijos, išskyrus naudotojo darbo dokumentus.

33.4. Naudotojams, savo tarnybinėms funkcijoms vykdyti, leidžiama naudoti tik su IS saugos įgaliotiniu suderintus belaidžio tinklo įrenginius, atitinkančius techninius kibernetinio saugumo reikalavimus.

34. Perkant paslaugas, darbus ar įrangą, susijusius su IS, jų projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, pirkimo dokumentuose turi būti nustatyta, kad paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas turi užtikrinti atitiktį kibernetinio saugumo reikalavimams.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

35. Kvalifikacijos ir patirties reikalavimai IS naudotojams, IS administratoriui, IS saugos įgaliotiniui:

35.1. IS naudotojai privalo turėti pagrindinių darbo kompiuteriu, taikomosiomis programomis įgūdžių, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją (įskaitant asmens duomenis ir komercinę paslaptį sudarančią informaciją), privalo neatskleisti jų trečiosioms šalims ir saugoti jų slaptumą, išskyrus įstatymų numatytas išimtis.

35.2. IS saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, tobulinti kvalifikaciją elektroninės informacijos saugos ir kibernetinio saugumo srityje, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos

reikalavimų aprašu ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą ir kibernetinį saugumą.

35.3. IS administratorius pagal kompetenciją privalo išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, mokėti užtikrinti IS ir elektroninės informacijos saugą ir kibernetinį saugumą, administruoti ir prižiūrėti komponentus (stebėti komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti IS komponentų nepertraukiamą funkcionavimą ir panašiai). IS administratorius turi būti susipažinęs su Saugos dokumentais.

36. IS saugos įgaliotiniu ir IS 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.

37. IS naudotojų ir IS administratoriaus mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo dažnumo reikalavimai:

37.1. IS naudotojams turi būti organizuojami mokymai elektroninės informacijos saugos ir kibernetinio saugumo klausimais, įvairiais būdais primenama apie elektroninės informacijos saugos ir kibernetinio saugumo problemas (pavyzdžiui, svarbios informacijos priminimai elektroniniu paštu, informacijos skelbimas Tarnybos vidiniame tinkle, lankstinukai–atmintinės ir panašiai).

37.2. Mokymai elektroninės informacijos saugos ir kibernetinio saugumo klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), IS naudotojų ir (ar) IS administratoriaus poreikius.

37.3. Mokymai gali būti vykdomi tiesioginiu (pavyzdžiui, paskaitos, seminarai, konferencijos ir kiti teminiai renginiai) ar nuotoliniu būdu (pavyzdžiui, vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir panašiai). Mokymus gali vykdyti IS saugos įgaliotinis ar kitas darbuotojas, išmanantis elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus, arba elektroninės informacijos saugos ir kibernetinio saugumo mokymų paslaugų teikėjas.

37.4. Mokymai IS naudotojams elektroninės informacijos saugos ir kibernetinio saugumo klausimais turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per dvejus metus. Mokymai IS administratoriui turi būti organizuojami pagal poreikį. Už mokymų organizavimą atsakingas IS saugos įgaliotinis.

V SKYRIUS
NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

38. Už IS naudotojų supažindinimą su Saugos dokumentais ir teisės aktais, kuriais vadovaujamasi tvarkant elektroninę informaciją, užtikrinant jos saugumą, ir atsakomybe už juose nustatytų reikalavimų nesilaikymą yra atsakingas IS saugos įgaliotinis.

39. IS naudotojai su Saugos dokumentais supažindinami elektroniniu būdu.

40. IS naudotojai pakartotinai supažindinami su Saugos dokumentais tik jiems iš esmės pasikeitus.

41. Tvarkyti elektroninę informaciją gali tik tie asmenys, kurie yra susipažinę su Saugos dokumentais ir įsipareigoję laikytis jų reikalavimų.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. IS saugos įgaliotinis turi ne rečiau kaip kartą per kalendorinius metus peržiūrėti Saugos dokumentus. Saugos dokumentai turi būti peržiūrimi atlikus IS rizikos vertinimą ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminių organizacinių, sisteminių ar kitų IS pokyčių.

43. Saugos dokumentų ir kitos su elektroninės informacijos sauga ir kibernetiniu saugumu susijusios dokumentacijos priežiūrą ar keitimą inicijuoja IS saugos įgaliotinis.

44. Naudotojai atsako už IS ir jose tvarkomos elektroninės informacijos saugą ir kibernetinį saugumą pagal savo kompetenciją.

45. Asmenys, pažeidę Saugos nuostatus, atsako teisės aktų nustatyta tvarka.

_____

Lietuvos Respublikos ryšių reguliavimo tarnybos
informacinių sistemų saugos nuostatų
priedas

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS VALSTYBĖS INFORMACINIŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	Valstybės informacinės sistemos pavadinimas	Elektroninės informacijos svarbos kategorija	Valstybės informacinės sistemos kategorija	Elektroninės informacijos ir valstybės informacinės sistemos priskyrimo atitinkamai kategorijai kriterijai
1.	Operatorių tinklų informacinė sistema	vidutinės svarbos	3	Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo (toliau – Klasifikavimo gairių aprašas) 9.1, 9.2 ir 12.3 papunkčiai
2.	Periodinių ataskaitų teikimo informacinė sistema	vidutinės svarbos	3	Klasifikavimo gairių aprašo 9.1, 9.2 ir 12.3 papunkčiai
3.	Radijo dažnių spektro valdymo informacinė sistema	vidutinės svarbos	3	Klasifikavimo gairių aprašo 9.1, 9.2 ir 12.3 papunkčiai
4.	Numerių ir kodų valdymo bei teisės vartoti domenus su Lietuvos vardu ir Elektroninių ryšių paslaugų ir tinklų teikėjų sąrašo administravimo informacinė sistema	vidutinės svarbos	3	Klasifikavimo gairių aprašo 9.1, 9.2 ir 12.3 papunkčiai

---

Priedo pakeitimai:
Nr. (1.9E)1V-51, 2021-01-13, paskelbta TAR 2021-01-19, i. k. 2021-00851

PATVIRTINTA
Lietuvos Respublikos ryšių reguliavimo
tarnybos direktoriaus 2019 m. vasario 26 d.
įsakymu Nr. 1V-240

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) nustato minimalius Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – Tarnybos) valdomose informacinėse sistemose (toliau – IS) tvarkomos elektroninės informacijos saugos reikalavimus.

2. Taisyklėse vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo 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“, ir 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 “.

3. Taisyklės taikomos Tarnybos valdomoms valstybės ir vidaus administravimo IS.

4. Taisyklės privalomos IS naudotojams, IS administratoriui, duomenų valdymo įgaliotiniui ir IS saugos įgaliotiniui.

5. Už Taisyklių įgyvendinimo organizavimą ir kontrolę atsako IS saugos įgaliotinis.

6. IS tvarkoma elektroninė informacija, nurodyta:

6.1. Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos nuostatų, patvirtintų Tarnybos direktoriaus 2016 m. rugsėjo 26 d. įsakymu Nr. 1V-1005 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninių paslaugų informacinės sistemos nuostatų patvirtinimo“, III skyriuje;

6.2. Radijo dažnių spektro valdymo informacinės sistemos nuostatų, patvirtintų Tarnybos direktoriaus 2006 m. balandžio 10 d. įsakymu Nr. 1V-507 „Dėl Radijo dažnių spektro valdymo informacinės sistemos nuostatų patvirtinimo“, III skyriuje;

6.3. Numerių ir kodų valdymo bei teisės vartoti domenus su Lietuvos vardu ir Elektroninių ryšių paslaugų ir tinklų teikėjų sąrašo administravimo informacinės sistemos nuostatų, patvirtintų Tarnybos direktoriaus 2015 m. gegužės 29 d. įsakymu Nr. 1V-656 „Dėl Numerių ir kodų valdymo bei teisės vartoti domenus su Lietuvos vardu ir Elektroninių ryšių paslaugų ir tinklų teikėjų sąrašo administravimo informacinės sistemos nuostatų patvirtinimo“, III skyriuje.

7. IS administratorius yra atsakingas už IS klasifikatorių, IS naudotojų duomenų ir jiems suteiktų teisių tvarkymą.

8. IS naudotojai yra atsakingi už duomenų, nurodytų Taisyklių 6 punkte, išskyrus nurodytus Taisyklių 7 punkte, tvarkymą.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

9. Bendrieji techniniai elektroninės informacijos saugos reikalavimai:

9.1. Periodiškai (ne rečiau kaip kartą per dvejus metus) turi būti atliekamas informacinių technologijų saugos atitikties vertinimas (toliau – auditas). Už audito administravimą ir audito ataskaitų saugojimą yra atsakingas Tarnybos Administracinio departamento Informacinių technologijų skyrius.

9.2. IS turi registruoti duomenų bazės informacijos ir tarnybinių stočių operacinės sistemos pakeitimus, fiksuoti paskutinį elektroninės informacijos pakeitimą atlikusį IS naudotoją ir tokio pakeitimo laiką.

9.3. IS priežiūros funkcijos turi būti vykdomos naudojant atskirą tam skirtą IS administratoriaus identifikatorių, kuriuo naudojantis negalima atlikti kitų IS naudotojų funkcijų.

9.4. Kiekvienas IS naudotojas turi būti unikaliai identifikuojamas – IS naudotojas patvirtina savo tapatybę kvalifikuotu sertifikatu.

9.5. IS naudotojui ar IS administratoriui baigus darbą su IS, turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo IS, saugi sertifikato laikmena atjungiama nuo kompiuterinės įrangos, uždaroma programinė įranga, įjungiama ekrano užsklanda su slaptažodžiu.

9.6. IS naudotojui neatliekant jokių veiksmų 60 min., IS naudotojo paskyra automatiškai atjungiama ir naudotis IS galima tik pakartojus IS naudotojo tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus.

9.7. IS turi perspėti IS administratorių, kai tarnybinėse stotyse laisvos operatyviosios atminties ar laisvos vietos diske sumažėja iki nustatytos pavojingos ribos, taip pat kai ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja.

9.8. IS turi būti įdiegtos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemonės (filtrai).

9.9. Tarnybinių stočių įvykių žurnaluose (angl. *event log*) turi būti fiksuojami ir vieną mėnesį saugomi duomenys apie: įjungimą, išjungimą, sėkmingus ir nesėkmingus bandymus registruotis ir prieiti prie IS elektroninės informacijos, kitus svarbius saugai įvykius, nurodant IS naudotojo identifikatorių ir įvykio laiką. Ši informacija analizuojama įvykus elektroninės informacijos saugos incidentui.

9.10. IS veiklos atkūrimas turi būti atliekamas vadovaujantis Tarnybos IS veiklos tęstinumo valdymo planu.

10. Kompiuterinės įrangos saugos priemonės:

10.1. Tarnybinės stotys ir svarbiausi elektroninės informacijos perdavimo tinklo mazgai turi įtampos filtrą ir nenutrūkstamo maitinimo šaltinį. Nenutrūkstamo maitinimo šaltinis užtikrina tarnybinių stočių veikimą ne trumpiau kaip 30 min.

10.2. Tarnybinės stotys, svarbiausi elektroninės informacijos perdavimo tinklo mazgai ir ryšio linijos yra dubliuojami ir jų techninė būklė nuolat stebima.

10.3. Kompiuterinės įrangos gedimai fiksuojami žurnale.

10.4. Visose tarnybinėse stotyse ir kompiuterizuotose darbo vietose yra įdiegta ir reguliariai atnaujinama virusų ir kenkimo kodo aptikimo ir šalinimo programinė įranga, skirta kompiuteriams ir laikmenoms tikrinti. Kompiuterizuotose darbo vietose naudojamos centralizuotai valdomos kenkimo programinės įrangos aptikimo priemonės, kurios reguliariai atnaujinamos.

11. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

11.1. Operacinei sistemai ir kitai programinei įrangai operatyviai atnaujinti naudojama WSUS (angl. *Windows Server Update Services*) tarnybinė stotis. Įdiegiami tik gamintojų rekomenduojami naujiniai.

11.2. Naudojama tik teisėtai įgyta, patikimų gamintojų programinė įranga.

11.3. Programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka tik IS administratorius.

11.4. Programinė įranga prižiūrima laikantis gamintojo rekomendacijų.

11.5. Programinės įrangos testavimas atliekamas naudojant atskirą testavimo aplinką.

12. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

12.1. Tarnybinės stotys, IS naudotojų kompiuterizuotos darbo vietos ir kita kompiuterinė įranga, įjungta į elektroninės informacijos perdavimo tinklą, yra atskirta nuo viešųjų elektroninių ryšių tinklų naudojant užkardas.

12.2. Elektroninės informacijos perdavimo tinklas yra segmentuotas pagal IS sudedamųjų dalių atliekamas funkcijas ir turi priskirtus IP (angl. *Internet Protocol*) adresų intervalus:

12.2.1. Tarnybinių stočių tinklą sudaro taikomųjų programų tarnybinės stotys.

12.2.2. IS naudotojų kompiuterizuotų darbo vietų tinklus sudaro nutolusių IS naudotojų kompiuterinės darbo vietos ir kompiuterinė įranga.

12.2.3. Kūrimo, tobulinimo ir testavimo tinklą sudaro testavimo darbams naudojamos tarnybinės stotys ir duomenų bazių testavimo tarnybinės stotys.

12.2.4. Administratorių tinklą sudaro darbuotojų, turinčių IS ir (ar) tarnybinių stočių administratoriaus teises, kompiuterizuotos darbo vietos.

12.2.5. Elektroninės informacijos perdavimo tinklo aptarnavimo ir saugumo potinklį sudaro tinklo stebėjimo, aptarnavimo, antivirusinių sistemų tarnybinės stotys.

12.2.6. Demilitarizuotos zonos tinklą sudaro tarnybinės stotys, kurios turi ryšį su viešaisiais elektroninių ryšių tinklais.

12.3. Demilitarizuota zona tiek nuo išorinio, tiek nuo vidinio elektroninės informacijos perdavimo tinklo atskirta užkardomis.

12.4. Nutolę IS naudotojai perduoda informaciją naudodami saugias ryšio linijas.

12.5. Nutolę IS naudotojai, duomenis perduodantys ir gaunantys viešaisiais elektroninių ryšių tinklais, perduodamų duomenų konfidencialumą užtikrina naudodami duomenų šifravimą arba virtualųjį privatųjį tinklą.

12.6. IS taikoma trijų lygių elektroninės informacijos perdavimo tinklo apsauga – išorinis tinklas, taikomosios programos, duomenų bazės, kiekvieną iš lygių atskiriant užkardomis.

12.7. Jungimasis prie IS iš viešųjų elektroninių ryšių tinklų yra griežtai kontroliuojamas ir atliekamas tik per tarpines tarnybines stotis.

12.8. Keitimasis informacija su registrais ir kitomis IS galimas tik naudojant saugius šifruotus ryšio kanalus (VPN (angl. *Virtual Private Network*), SSL (angl. *Secure Sockets Layer*)) ir tarpines tarnybines stotis.

12.9. Elektroninės informacijos perdavimo tinklai stebimi šia tvarka:

12.9.1. Visi tinklo įrenginiai, turintys paprastojo tinklo stebėjimo protokolo (angl. *Simple Network Management Protocol, SNMP*) parinktį, stebimi tinklo priežiūros sistemos ir, kilus nesklandumų, automatiškai praneša apie problemą atsakingiems darbuotojams.

12.9.2. Visi ryšių kanalai stebimi tinklo priežiūros sistemos ir, esant sutrikimų arba didelei apkrovai, automatiškai praneša apie problemą atsakingiems darbuotojams.

12.9.3. Duomenų gavėjams duomenys viešaisiais elektroninių ryšių tinklais perduodami tik saugiu hipertekstų persiuntimo protokolu (angl. *Hypertext Transfer Protocol Secure, HTTPS*).

13. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

13.1. Tarnybos pastate įrengta elektroninė perimetro kontrolės sistema. Tarnybinių stočių patalpos turi atskirą elektroninę perimetro kontrolės sistemą.

13.2. Tarnybos pastate įrengta atskirų patalpų apsaugos signalizacija, kurios signalai pasibaigus darbo dienai, taip pat poilsio ir švenčių dienomis persiunčiami patalpas saugančiai saugos tarnybai. Visose patalpose įrengti įsilaužimo davikliai prijungti prie pastato signalizacijos ir apsaugos tarnybos.

13.3. Kiekvienas darbuotojas turi asmeninę magnetinę kortelę ir įeidamas arba išeidamas pasižymi įėjimo punktuose.

13.4. Visi darbuotojų įėjimai į patalpas ir išėjimai fiksuojami ir saugomi elektronine forma.

13.5. Lankytojams privalomai išduodamos svečio elektroninės kortelės. Už apsilankymą atsakingas darbuotojas pasirašo įėjimo žurnale už kiekvieną lankytoją.

13.6. Po 18 val. vakaro ir nedarbo dienomis į pastatą patekti gali tiktai specialius leidimus turintys darbuotojai.

13.7. Tarnybinių stočių patalpos sienos sumūrytos iš plytų ar blokelių, lubos pagamintos iš gelžbetonio.

13.8. Tarnybinių stočių patalpos durys atsparios laužimui, nedegios, savaime užsidarančios. Duryse yra viena cilindrinė spyna ir viena plokštelinė spyna.

13.9. Į tarnybinių stočių patalpas gali patekti tik Tarnybos direktoriaus patvirtintame sąraše išvardyti darbuotojai. Valymas, elektros tinklo priežiūra, patalpų remonto ir kiti darbai atliekami tik dalyvaujant darbuotojui, turinčiam leidimą patekti į tarnybinių stočių patalpas.

13.10. Tarnybinių stočių patalpa turi alternatyvų elektros energijos tiekimo šaltinį.

13.11. Nenutrūkstamo maitinimo šaltinis vieną kartą per mėnesį tikrinamas imituojant elektros energijos dingimą.

13.12. Nenutrūkstamo maitinimo šaltinis automatiškai įsijungia dingus elektros įtampai, o sistema automatiškai informuoja atsakingus darbuotojus apie gedimą.

13.13. Aplinkos drėgnis tarnybinių stočių patalpoje nuolat stebimas automatizuotos sistemos. Rodmenims padidėjus arba sumažėjus daugiau nei technikos gamintojo nurodytos leistinos normos, sistema automatiškai informuoja atsakingus darbuotojus apie nesklandumus.

13.14. Tarnybinių stočių patalpoje įrengta gaisro gesinimo dujomis sistema.

13.15. Kitose patalpose prieinamoje vietoje įrengtos nešiojamosios gaisro gesinimo priemonės ir gaisriniai čiaupai.

13.16. Visos priešgaisrinės sistemos ir priemonės periodiškai tikrinamos kas mėnesį. Patikros užfiksuojamos žurnale, kuriame nurodoma patikros data, patikrinimo lygis, asmens, atlikusio patikrą, vardas, pavardė ir parašas.

13.17. Už priešgaisrinę saugą atsakingas Tarnybos Administracinio departamento Išteklių valdymo ir logistikos skyrius.

13.18. Tarnybinių stočių patalpos raktai saugomi seife. Atsarginiai tarnybinių stočių patalpos raktai saugomi kitame nei pagrindiniai raktai pastate.

13.19. Ribojama fizinė prieiga prie tinklo kabelių, skirstytuvų, atšakų, kartotuvų ir antgalių.

13.20. Kompiuterių ryšio linijos apsaugotos nuo elektros išlydžių, perkūnijos ir elektros linijų avarijų naudojant apsauginius įtaisus su įžeminimo tašku.

14. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

14.1. IS naudotojams suteikiama prieigos teisė atlikti veiksmus Tarnybos IS naudotojų administravimo taisyklėse nustatyta tvarka.

14.2. Elektroniniuose žurnaluose fiksuojami IS naudotojo veiksmai su IS duomenimis.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

15. Saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka:

15.1. IS tvarkomus duomenis įvesti, keisti, atnaujinti, naikinti gali IS naudotojas pagal jam Tarnybos IS naudotojų administravimo taisyklių nustatyta tvarka suteiktas teises.

15.2. IS duomenys gali būti įvesti, pakeisti, atnaujinti, sunaikinti tik turint tam teisinį pagrindą.

15.3. Duomenų įvedimas, keitimas, atnaujinimas, naikinimas fiksuojami elektroniniuose žurnaluose, nurodant IS naudotoją, veiksmų atlikimo laiką, prisijungimo prie IS datą, atliktus veiksmus.

16. IS naudotojų veiksmų fiksavimo tvarka:

16.1. IS naudotojo veiksmai su duomenimis automatiškai registruojami elektroniniuose žurnaluose.

16.2. IS administratorius gali peržiūrėti duomenų sukūrimo, keitimo, atnaujinimo ar naikinimo veiksmus pagal atskirą objektą (pavyzdžiui, dokumentą, klasifikatorių), IS naudotoją, instituciją, laiko intervalą.

17. Atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka yra nustatyta Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninės informacijos atsarginio kopijavimo, atsarginių kopijų saugojimo ir atkūrimo iš atsarginių kopijų taisyklėse, patvirtintose Tarnybos direktoriaus 2018 m. gegužės 17 d. įsakymu Nr. 1V-477 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos elektroninės informacijos atsarginio kopijavimo, atsarginių kopijų saugojimo ir atkūrimo iš atsarginių kopijų taisyklių patvirtinimo“.

18. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo nustatymo tvarka:

18.1. IS naudotojai, pastebėję neteisėtą duomenų kopijavimą, keitimą, naikinimą, perdavimą ar kitus saugos reikalavimų pažeidimus, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai IS administratoriui.

18.2. IS administratorius jam prieinamomis priemonėmis patikrina gautą pranešimą apie pažeidimą ir, faktui pasitvirtinus, užfiksuoja incidentą elektroninės informacijos saugos incidentų žurnale ir imasi visų įmanomų priemonių pažeidimui užkirsti ar nutraukti.

19. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

19.1. Techninė ir programinė įranga atnaujinama pagal Taisyklių 20 punkte nurodytą IS pakeitimų valdymo tvarką.

19.2. Programinės ir techninės įrangos keitimo ir atnaujinimo tvarką su trečia šalimi, kuriai Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme nustatytomis sąlygomis ir tvarka perduotos IS ir (ar) jos infrastruktūros priežiūros funkcijos (toliau – paslaugų teikėjas), atsižvelgiant į konkretų atvejį, derina IS administratorius arba ji aprašoma paslaugų, susijusių su programinės ir techninės įrangos keitimu ir atnaujinimu, teikimo sutartyse ir priežiūros reglamentuose.

19.3. Perėjimą prie naujos operacinės sistemos versijos inicijuoja IS administratorius.

19.4. Apie visus darbus, kurie gali sutrikdyti IS veikimą, IS administratorius iš anksto privalo informuoti IS saugos įgaliotinį ir IS naudotojus.

20. IS pakeitimų valdymo tvarka:

20.1. IS pakeitimų valdymo planavimas apima IS pakeitimų identifikavimą, suskirstymą į kategorijas pagal IS pakeitimo tipą (administracinis, organizacinis ar techninis), poveikio vertinimą (svarbumas ir skubumas) ir IS pakeitimų prioritetų nustatymą.

20.2. Duomenų valdymo įgaliotinis, vadovaudamasis IS plėtros planu, kitais IS valdytojo planavimo dokumentais:

20.2.1. planuoja IS pakeitimų valdymą, kuris apima pakeitimų identifikavimą, suskirstymą į kategorijas pagal pakeitimo tipą (administracinis, organizacinis ar techninis);

20.2.2. siūlo Tarnybos direktoriui ar jo įgaliotam asmeniui IS pakeitimų poveikio vertinimą (svarbumas ir skubumas) ir IS pakeitimų prioritetą;

20.2.3. įgyvendina IS ar funkciškai savarankiškos jos sudedamosios dalies (toliau – posistemis) plėtrą;

20.2.4. tiesiogiai prižiūri, kaip kuriama ir tvarkoma IS, jos posistemiai, diegiama programinė įranga, panaudojamos investicijos;

20.2.5. rengia IS biudžeto projektus.

20.3. IS pakeitimai identifikuojami pasikeitus su IS veikla susijusiems teisės aktams, nustačius naujus IS naudotojų, IS administratoriaus poreikius, apibendrinus kylančias priežiūros problemas ir kitais gerosios praktikos įvardijamais atvejais.

20.4. IS pakeitimus turi teisę inicijuoti IS saugos įgaliotinis, IS administratorius ar duomenų valdymo įgaliotinis, o įgyvendinti – IS administratorius arba duomenų valdymo įgaliotinis pagal kompetenciją.

20.5. IS programinės įrangos pakeitimai atliekami tik įvertinus pakeitimų poreikį, pakeitimų apimtį.

20.6. IS funkcijų ir galimybių sąrankos aprašai turi būti nuolat atnaujinami ir atspindėti esamą IS sąrankos būklę.

20.7. IS pakeitimai įgyvendinami Tarnybos direktoriaus ar jo įgalioto asmens patvirtintu eiliškumu, atsižvelgiant į nustatytą skubumą ar svarbumą.

20.8. Visi diegiami IS pakeitimai, galintys sutrikdyti ar sustabdyti IS darbą, turi būti suderinti su duomenų valdymo įgaliotiniu bei IS saugos įgaliotiniu ir vykdomi tik gavus jų raštišką pritarimą.

20.9. Prieš atlikdamas IS pakeitimus, kurių metu gali iškilti grėsmė duomenų konfidencialumui, vientisumui ar pasiekiamumui, IS administratorius privalo įsitikinti, kad planuojami IS pakeitimai išbandyti testinėje aplinkoje.

20.10. Programinės įrangos testavimas atliekamas naudojant tam skirtą testinę aplinką, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos.

20.11. Atlikus planuojamų IS pakeitimų testavimą, IS administratorius gali pradėti įgyvendinti IS pakeitimus tik suderinęs tai su IS saugos įgaliotiniu.

20.12. Planuodamas IS pakeitimus, kurių metu galimi IS veikimo sutrikimai, IS administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki IS pakeitimų vykdymo pradžios informuoti IS naudotojus apie tokių darbų pradžią ir galimus IS veikimo sutrikimus.

21. Kompiuterių ir kitų mobiliųjų įrenginių naudojimo tvarka:

21.1. Nešiojamieji kompiuteriai ir mobilieji įrenginiai turi būti saugomi ir negali būti palikti be priežiūros viešose vietose.

21.2. Visi nešiojamieji kompiuteriai ir kiti mobilieji įrenginiai turi būti apsaugoti saugiais slaptažodžiais, sudėtingumu atitinkančiais Tarnybos IS naudotojų administravimo taisyklių reikalavimus.

22. Kiti reikalavimai yra nustatyti Lietuvos Respublikos ryšių reguliavimo tarnybos kompiuterių tinklo, kompiuterinės ir programinės įrangos naudojimo ir administravimo tvarkos apraše, patvirtintame Tarnybos direktoriaus 2018 m. spalio 2 d. įsakymu Nr. 1V-921 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos kompiuterių tinklo, kompiuterinės ir programinės įrangos naudojimo ir administravimo tvarkos aprašo patvirtinimo“.

IV SKYRIUS
REIKALAVIMAI IS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

23. Reikalavimai IS funkcionuoti reikalingoms paslaugoms ir jų teikėjams nustatomi paslaugų teikimo sutartyse.

24. IS administratorius atsako už programinių, techninių ir kitų prieigos prie IS išteklių priemonių organizavimą, suteikimą ir panaikinimą techninės ir (ar) programinės įrangos priežiūros paslaugos teikėjui.

25. IS administratorius suteikia paslaugos teikėjui tik tokią prieigą prie IS išteklių, kuri yra būtina norint įvykdyti paslaugų teikimo sutartyje nustatytus įsipareigojimus ir kuri neprieštarauja įstatymų ir kitų teisės aktų reikalavimams.

26. Su paslaugų teikėju turi būti suderinta paslaugos teikimo tvarka, į kurią įtraukti prieigos prie IS reikalavimai ir jos suteikimo sąlygos.

27. Pasibaigus sutarties su paslaugos teikėjais galiojimo terminui ar atsiradus paslaugų teikimo sutartyje ar saugos politiką įgyvendinančiuose dokumentuose įvardytų kitų sąlygų, IS administratorius nedelsdamas privalo panaikinti suteiktą prieigą.

28. Reikalavimai, keliami paslaugų teikėjų patalpoms, įrangai, priežiūrai, duomenų perdavimui tinklais ir kitoms paslaugoms, nurodomi paslaugų teikimo sutartyse.

29. Paslaugų teikėjų darbuotojams, atliekantiems IS administravimo funkcijas, taikomi visi IS administratoriui Tarnybos IS saugos politikos įgyvendinamuosiuose dokumentuose nustatyti reikalavimai.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

30. Asmenys, pažeidę Taisyklių reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

PATVIRTINTA
Lietuvos Respublikos ryšių reguliavimo
tarnybos direktoriaus 2019 m. vasario 26 d.
įsakymu Nr. 1V-240

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų veiklos tęstinumo valdymo plane (toliau – Planas) nustatomos taisyklės ir procedūros, kurių būtina laikytis atkuriant Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – Tarnyba) informacinių sistemų (toliau – IS) veiklą įvykus elektroninės informacijos saugos incidentui, įskaitant kibernetinį incidentą (toliau – saugos incidentas).

2. Kibernetinių incidentų atveju, jų nustatymas, informavimas apie kibernetinius incidentus, kibernetinių incidentų tyrimas ir kibernetinių incidentų analizė baigus kibernetinių incidentų tyrimą, vykdomi Nacionaliniame kibernetinių incidentų valdymo plane, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, (toliau – Nacionalinis planas) nustatyta tvarka, o Plano nuostatos taikomos tiek, kiek kibernetinių incidentų valdymo nereglamentuoja Nacionalinis planas.

3. Planas taikomas įvykus saugos incidentui.

4. Plane vartojamos sąvokos apibrėžtos 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“.

5. Planas privalomas IS valdytojui, IS tvarkytojui, IS saugos įgaliotiniui, IS administratoriui, IS naudotojams.

6. IS veiklos atkūrimas įvykus saugos incidentui finansuojamas Lietuvos Respublikos valstybės biudžeto lėšomis iš Tarnybos įmokėtų pajamų įmokų.

7. IS administratorius, IS saugos įgaliotinis, prireikus – IS naudotojai, nedelsdami šalina saugos incidento padarinius ir įgyvendina kitas Plano 3 priede pateiktame Tarnybos IS veiklos tęstinumo detaliajame plane numatytas priemones.

8. Kriterijai, pagal kuriuos nustatoma, kad IS veikla atkurta:

8.1. nuolat atnaujinami IS duomenys;

8.2. išsaugomi atnaujinti IS duomenys;

8.3. IS gali naudotis visi IS naudotojai;

8.4. iš susijusių registrų ir IS gaunami duomenys yra atnaujinami ir išsaugomi.

9. IS veikla laikoma atkurta, jeigu IS yra vėl prieinama ne mažiau kaip 90 procentų laiko per parą.

10. Saugos incidento tyrimas atliekamas pagal Plano 1 priede pateiktą Tarnybos IS saugos incidentų valdymo tvarkos aprašą.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

11. Saugos incidentams valdyti ir IS veiklai atkurti sudaromos dvi grupės: IS veiklos tęstinumo valdymo grupė (toliau – valdymo grupė) ir IS veiklos atkūrimo grupė (toliau – veiklos atkūrimo grupė).

12. Valdymo grupės tikslai – tirti saugos incidentus, ieškoti priemonių ir būdų sukeltiems padariniams ir žalai likviduoti, užtikrinti IS veiklos tęstinumą.

13. Valdymo grupės sudėtis:

13.1. grupės vadovas – IS saugos įgaliotinis;

13.2. grupės vadovo pavaduotojas – Tarnybos Administracinio departamento Informacinių technologijų skyriaus (toliau – IT skyrius) vedėjas;

13.3. grupės nariai – IT skyriaus darbuotojai.

14. Valdymo grupės funkcijos:

14.1. situacijos analizė, problemų (saugos incidentų) nustatymas;

14.2. sprendimų IS veiklos tęstinumo valdymo klausimais priėmimas ir jų vykdymo kontrolė;

14.3. bendravimas su teisėsaugos ir kitomis institucijomis, IS naudotojų informavimas;

14.4. finansinių ir kitų išteklių, reikalingų IS veiklai atkurti, įvykus saugos incidentui, nustatymas ir naudojimo kontrolė;

14.5. elektroninės informacijos fizinės saugos, įvykus saugos incidentui, užtikrinimas;

14.6. logistikos (žmonių, daiktų, įrangos gabenimo) organizavimas;

14.7. bendravimas su kitų IS veiklos tęstinumo valdymo grupėmis;

14.8. IS veiklos atkūrimo priežiūra ir koordinavimas.

15. Veiklos atkūrimo grupės tikslas – likviduoti saugos incidentus.

16. Veiklos atkūrimo grupę sudaro:

16.1. grupės vadovas – IS saugos įgaliotinis;

16.2. grupės vadovo pavaduotojas – IT skyriaus vedėjas;

16.3. grupės nariai – IT skyriaus darbuotojai.

17. Veiklos atkūrimo grupės funkcijos:

17.1. tarnybinių stočių veikimo atkūrimo organizavimas;

17.2. kompiuterių tinklo veikimo atkūrimo organizavimas;

17.3. taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

17.4. kompiuterizuotų darbo vietų veikimo atkūrimo ir prijungimo prie kompiuterių tinklo organizavimas;

17.5. IS elektroninės informacijos atkūrimo organizavimas.

18. Valdymo grupės ir veiklos atkūrimo grupės sudėtys yra tvirtinamos Tarnybos direktorius įsakymu.

19. Įvykus saugos incidentui, valdymo grupės vadovas organizuoja valdymo grupės susirinkimą.

20. Valdymo grupė, atlikusi situacijos analizę, susisiekia su veiklos atkūrimo grupe ir informuoja apie esamą padėtį bei priimtus sprendimus dėl veiklos atkūrimo.

21. Valdymo grupės ir veiklos atkūrimo grupės nariai tarpusavyje bendrauja asmeniškai, elektroniniu paštu, telefonu ir kitomis ryšio priemonėmis.

22. IS veiklos atkūrimo veiksmai ir už jų vykdymą atsakingi asmenys nurodyti Plano 3 priede pateiktame Tarnybos IS veiklos tęstinumo detaliajame plane.

23. Apie įvykdytus IS veiklos atkūrimo veiksmus atsakingi asmenys nedelsdami informuoja veiklos atkūrimo grupės vadovą.

24. Veiklos atkūrimo grupės vadovas nuolat informuoja valdymo grupės narius apie IS veiklos atkūrimo eigą.

25. Atsarginėms patalpoms, naudojamoms IS veiklai atkurti saugos incidento metu, esančioms adresu: Sausio 13-osios g. 10, LT-04347 Vilnius, keliami šie reikalavimai:

25.1. Patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų.

25.2. Patalpose turi būti įrengta langų ir durų fizinė apsauga.

25.3. Patalpos turi atitikti priešgaisrinės saugos reikalavimus, jose turi būti gaisro gesinimo priemonės.

25.4. Ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo prie jų ir pažeidimo.

25.5. Turi būti įgyvendintos gamintojo nustatytos techninės įrangos veikimo sąlygos.

25.6. Patalpose turi būti užtikrintas patikimas elektros energijos tiekimas per nenutrūkstamo maitinimo šaltinius.

25.7. Patalpose turi būti užtikrinta interneto prieiga.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

26. Kompiuterinės ir programinės įrangos sąrašai, šios įrangos parametrai ir už jos priežiūrą atsakingi asmenys nurodyti elektroniniame žurnale, kurį tvarko ir saugo IS administratorius. Laikinai nesant IS administratoriaus, jį gali pavaduoti kitas, Tarnybos direktoriaus įsakymu paskirtas, Tarnybos darbuotojas, atitinkantis Tarnybos IS saugos politiką įgyvendinančiuose dokumentuose IS administratoriui nustatytus reikalavimus.

27. Tarnybos pastato, kuriame yra IS tarnybinės stotys, aukšto planas saugomas Tarnybos Administracinio departamento Turto valdymo ir logistikos skyriuje.

28. Tarnybos patalpose esančios įrangos ir komunikacijų brėžiniai saugomi IT skyriuje.

29. Duomenų teikimo ir pagrindinės kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašai saugomi IT skyriuje.

30. Programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis žurnalas, kuriame nurodoma programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos, saugomas IT skyriuje.

31. Valdymo grupės ir veiklos atkūrimo grupės narių telefono ryšio numeriai skelbiami Tarnybos interneto svetainėje ir saugomi IS saugos įgaliotinio.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

32. Plano veiksmingumas turi būti išbandytas per šešis mėnesius nuo jo patvirtinimo dienos. Plano veiksmingumas turi būti išbandomas ne rečiau kaip kartą per metus, modeliuojant saugos incidentą.

33. Išbandymo rezultatai nurodomi Plano 4 priede pateiktos formos Plano veiksmingumo išbandymo ataskaitoje, kurią parengia IS saugos įgaliotinis kartu su IS administratoriumi. Už Plano veiksmingumo išbandymo ataskaitos pateikimą Tarnybos direktoriui ar jo įgaliotam asmeniui atsakingas IS saugos įgaliotinis.

34. Plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami vadovaujantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

_____

Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų veiklos tęstinumo valdymo plano
1 priedas

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS INFORMACINIŲ SISTEMŲ SAUGOS INCIDENTŲ VALDYMO TVARKOS APRAŠAS

1. IS naudotojai, pastebėję Tarnybos IS saugos politiką įgyvendinančių dokumentų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami apie tai pranešti IS administratoriui.

2. IS administratorius nedelsdamas turi imtis veiksmų, reikalingų saugos incidentui stabdyti, padariniams likviduoti, ir apie tai pranešti IS saugos įgaliotiniui, kuris, įvertinęs saugos incidento reikšmingumą, informuoja valdymo grupės vadovą.

3. IS saugos įgaliotinis su IS administratoriumi nagrinėja saugos incidentą, priskiria jį tam tikrai klasei ir priima sprendimą dėl saugos incidento svarbos lygio.

4. IS administratorius, suderinęs su IS saugos įgaliotiniu, atlieka neatidėliotinus administravimo veiksmus, skirtus saugos incidento plėtrai sustabdyti ir jo tyrimui būtinai informacijai surinkti.

5. IS administratorius surenka visą su saugos incidentu susijusią informaciją ir įvykį fiksuoja Plano 2 priede pateiktos formos Tarnybos IS saugos incidentų žurnale, nurodydamas incidento vietą, laiką, pobūdį, IS atkuriamuosius darbus ir kitą su saugos incidentu susijusią informaciją, informuoja apie saugos incidentą pranešusį asmenį apie pašalintus saugos incidento sukeltus nesklandumus.

6. Saugos incidentui paveikus kitas, ne Tarnybos valdomas IS, IS administratorius informuoja saugos incidento poveikį patyrusius ar galinčius patirti paslaugų teikėjus ir (ar) kitas institucijas, atsižvelgia į jų rekomendacijas ir vykdo jų nurodymus.

7. Valdymo grupės vadovas, atsižvelgdamas į saugos incidento pobūdį, gali inicijuoti jo išsamų tyrimą.

8. Nusprendęs pradėti saugos incidento tyrimą, valdymo grupės vadovas teikia Tarnybos direktoriui siūlymą sudaryti atskirą tyrimo komisiją, kuri per penkiolika darbo dienų turi:

8.1. ištirti saugos incidento atsiradimo priežastis;

8.2. nustatyti asmenis, dėl kurių veiksmų ir (ar) neveikimo įvyko saugos incidentas;

8.3. nustatyti saugos incidento pasekmes ar dėl jo atsiradusią žalą;

8.4. parengti ir pateikti valdymo grupės vadovui tyrimo išvadas.

9. Valdymo grupės vadovas, atsižvelgdamas į tyrimo komisijos pateiktas išvadas, turi teisę teikti Tarnybos direktoriui siūlymus dėl atsakomybės taikymo teisės aktų nustatyta tvarka.

_____

Lietuvos Respublikos ryšių reguliavimo tarnybos
informacinių sistemų veiklos tęstinumo valdymo
plano
2 priedas

(Saugos incidentų apskaitos žurnalo forma)

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS INFORMACINIŲ SISTEMŲ SAUGOS INCIDENTŲ ŽURNALAS

Eil. Nr.	**Elektroninės informacijos saugos incidentas**						
	Informacinės sistemos naudotojo padalinio pavadinimas	**Požymio kodas***	**Elektroninės informacijos saugos incidento aprašymas**	**Pradžia (metai, mėnuo, diena, valanda)**	**Pabaiga (metai, mėnuo, diena, valanda)**	**Elektroninės informacijos saugos incidentą pašalinusio (-ių) darbuotojo (-ų) v. pavardė (-ės)**	**Informacinės sistemos saugos įgaliotinis (v. pavardė, parašas)**
1	2	3	4	5	6	7	8

* Elektroninės informacijos saugos incidento požymių kodai:
1 – gamtos reiškiniai; 2 – gaisras; 3 – elektros energijos tiekimo sutrikimai; 4 – vandentiekio ir šildymo sistemų sutrikimai; 5 – ryšio sutrikimai; 6 – įsilaužimas į vidinį kompiuterių tinklą; 7 – pagrindinių tarnybinių stočių sugadinimas ir (ar) praradimas; 8 – vagystė iš duomenų bazės ar jos fizinis sunaikinimas; 9 – programinės įrangos sugadinimas, praradimas; 10 – pavojingas (įtartinas) radinys; 11 – įvykis, susijęs su teroristine veikla; 12 – dokumentų praradimas; 13 – dalinis informacinės sistemos sutrikimas dėl neaiškių priežasčių.

_____

Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų veiklos tęstinumo valdymo plano
3 priedas

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO DETALUSIS PLANAS

Eil. Nr.	**Elektroninės informacijos saugos incidentas**	**Pirmaeiliai veiksmai**	**Pasekmių likvidavimo veiksmai**	**Terminai**	**Atsakingi vykdytojai**
1	2	3	4	5	6
1.	Gamtos reiškiniai (potvynis, uraganas ir kiti)	1.1. Elektroninės informacijos saugos incidento padarinių įvertinimas, priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas ir įgyvendinimas	1.1.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Per 15 min. nuo incidento nustatymo	Valdymo grupės vadovas
			1.1.2. Priemonių plano pavojui sustabdyti ir padarytai žalai likviduoti sudarymas	Per 30 min. nuo incidento nustatymo	Valdymo grupės vadovas
			1.1.3. Darbuotojų informavimas, padarytą žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	IS saugos įgaliotinis
			1.1.4. Elektroninės informacijos saugos incidento metu padarytos žalos likvidavimas, pirmosios pagalbos suteikimas nukentėjusiems darbuotojams	Nedelsiant	IS administratorius
2.	Gaisras	2.1. Priešgaisrinės gelbėjimo tarnybos informavimas	2.1.1. Įvykio vietos lokalizavimas, jei Priešgaisrinė gelbėjimo tarnyba rekomenduoja	Nedelsiant	IS saugos įgaliotinis

		2.2. Gaisro gesinimas ankstyvoje stadijoje, jei yra rekomendacija dirbti pavojaus zonoje	2.2.1. Galimybių evakuoti darbuotojus įvertinimas, jei Priešgaisrinė gelbėjimo tarnyba rekomenduoja	Nedelsiant	Valdymo grupės vadovas, IS saugos įgaliotinis
		2.3. Darbas pavojaus zonoje, komunikacijų, sukeliančių pavojų, išjungimas	2.3.1. Darbuotojų informavimas apie evakavimą, jei Priešgaisrinė gelbėjimo tarnyba rekomenduoja	Nedelsiant	IS saugos įgaliotinis
		2.4. Sutrikimų pašalinimas	2.4.1. Darbuotojų informavimas apie saugų darbą pavojaus zonoje	Nedelsiant	IS saugos įgaliotinis
			2.4.2 Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
			2.4.3. Padarytą žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	IS saugos įgaliotinis
			2.4.4. Elektroninės informacijos saugos incidento metu padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	IS administratorius
3.	Elektros energijos tiekimo sutrikimai	3.1. Elektros energijos tiekimo sutrikimo priežasčių nustatymas	3.1.1. Rekomendacijų iš elektros energijos tiekimo tarnybos gavimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
		3.2. Tarnybinių stočių, kitos techninės įrangos maitinimo išjungimas	3.2.1. Padarytos žalos įvertinimas	Per 1,5 val. nuo incidento nustatymo	Valdymo grupės vadovas
		3.3. Kreipimasis į elektros energijos tiekimo tarnybą dėl pavojaus trukmės ir sutrikimo pašalinimo galimybių	3.3.1. Žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	IS saugos įgaliotinis

		3.4. Sutrikimų pašalinimas	3.4.1. Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	IS saugos įgaliotinis, IS administratorius, valdymo grupės vadovas
4.	Vandentiekio ir šildymo sistemų sutrikimai	4.1. Vandentiekio ir šildymo paslaugų teikėjų informavimas	4.1.1. Paslaugų teikėjų rekomendacijų gavimas	Per 1 val. nuo incidento nustatymo	Veiklos grupės vadovas
			4.1.2. Darbuotojų informavimas apie rekomendacijas	Iš karto po rekomendacijų gavimo	IS saugos įgaliotinis
		4.2. Sutrikimo šalinimo prognozės skelbimas	4.2.1. Padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Veiklos grupės vadovas
			4.2.2. Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	Veiklos grupės vadovas
5.	Elektroninių ryšių tinklo sutrikimas	5.1. Elektroninių ryšių sutrikimo priežasčių nustatymas	5.1.1. Ryšio paslaugos teikėjo rekomendacijų gavimas	Per 1 val. nuo incidento nustatymo	IS administratorius
		5.2. Elektroninių ryšių paslaugų teikėjų informavimas, sutrikimo trukmės ir šalinimo prognozavimas	5.2.1. Sutrikimo likvidavimas	Priklausomai nuo atkūrimo darbų apimties	IS administratorius
6.	Įsilaužimas į vidinį kompiuterių tinklą	6.1. Pranešimas teisėsaugos institucijai apie įvykį	6.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	IS saugos įgaliotinis
		6.2. Priemonių plano sudarymas ir įgyvendinimas	6.2.1. Elektroninės informacijos saugos incidento pasekmių likvidavimas	Nedelsiant	IS administratorius
7.	Pagrindinių tarnybinių stočių sugadinimas ir	7.1. Pranešimas teisėsaugos institucijai apie įvykį	7.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas

	(ar) praradimas	7.2. Priemonių plano sudarymas ir įgyvendinimas	7.2.1. Padarytą žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	IS saugos įgaliotinis
			7.2.2. Elektroninės informacijos saugos incidento pasekmių likvidavimas	Priklausomai nuo atkūrimo darbų apimties	IS administratorius
			7.2.3. Padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
			7.2.4. Žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	Valdymo grupės vadovas
8.	Vagystė iš duomenų bazės ar jos fizinis sunaikinimas	8.1. Pranešimas teisėsaugos institucijai apie įvykį	8.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas
		8.2. Priemonių plano sudarymas ir įgyvendinimas	8.2.1. Padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
			8.2.2. Duomenų atkūrimas iš atsarginių kopijų	Per 8 val.	IS administratorius
9.	Programinės įrangos sugadinimas, praradimas	9.1. Pranešimas teisėsaugos institucijai apie įvykį	9.1.1. Teisėsaugos institucijos nurodymų vykdymas, priemonių plano sudarymas ir įgyvendinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
		9.2. Programinės įrangos kopijų periodinis gaminimas	9.2.1. Elektroninės informacijos saugos incidento metu padarytos žalos įvertinimas	Per 1 val. nuo incidento nustatymo	Valdymo grupės vadovas
			9.2.2. Žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	IS saugos įgaliotinis
			9.2.3. Padarytos žalos likvidavimas	Priklausomai nuo atkūrimo darbų apimties	IS administratorius
10.	Pavojingas (įtartinas) radinys	10.1. Pranešimas teisėsaugos institucijai apie įvykį	10.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas

11.	Įvykis, susijęs su teroristine veikla	11.1. Pranešimas teisėsaugos institucijai apie įvykį	11.1.1. Teisėsaugos institucijos nurodymų vykdymas	Nedelsiant	Valdymo grupės vadovas
		11.2. Darbuotojų evakavimas, jei yra rekomendacija	11.2.1. Darbuotojų informavimas apie nurodymų vykdymą	Nedelsiant	IS saugos įgaliotinis
12.	Dokumentų praradimas	12.1. Vadovybės informavimas	12.1.1. Prarastų dokumentų atkūrimas	Per 8 val. nuo incidento nustatymo	IS saugos įgaliotinis
13.	Dalinis informacinės sistemos veiklos sutrikimas dėl nenustatytų priežasčių	13.1. Atsakingų darbuotojų informavimas, Techninių specialistų pasitarimo problemai nustatyti organizavimas	13.1.1. Padarytos žalos įvertinimas	Nedelsiant	IS saugos įgaliotinis
		13.2. Problemos lokalizavimas	13.2.1. Padarytą žalą likviduojančių darbuotojų instruktavimas	Nedelsiant	IS administratorius
		13.3. Problemos šalinimas	13.3.1. Elektroninės informacijos saugos incidento pasekmių likvidavimas	Nedelsiant	Valdymo grupės vadovas

_____

Lietuvos Respublikos ryšių reguliavimo tarnybos
informacinių sistemų veiklos tęstinumo valdymo
plano
4 priedas

(Plano veiksmingumo išbandymo ataskaitos forma)

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO ATASKAITA

_____ Nr.
(data)

1. Plano išbandymo data:
2. Bandyme dalyvavo:

_____
(pareigos, vardas, pavardė)

3. Elektroninės informacijos saugos incidento scenarijus:

_____

4. Funkcijos ir posistemiai, kuriuos paveikė elektroninės informacijos saugos incidentas:

_____

5. Elektroninės informacijos saugos incidento šalinimo eiga:

_____

6. Rasti trūkumai:

_____

7. Pasiūlymai keisti arba papildyti planą:

_____

Informacinių sistemų saugos įgaliotinis:

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

Informacinių sistemų administratorius:

_____	_____	_____
(pareigos)	(parašas)	(vardas ir pavardė)

PATVIRTINTA
Lietuvos Respublikos ryšių reguliavimo
tarnybos direktoriaus 2019 m. vasario 26 d.
įsakymu Nr. 1V-240

LIETUVOS RESPUBLIKOS RYŠIŲ REGULIAVIMO TARNYBOS INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų naudotojų administravimo taisyklės (toliau – Taisyklės) reglamentuoja Lietuvos Respublikos ryšių reguliavimo tarnybos (toliau – Tarnyba) informacinių sistemų (toliau – IS) naudotojų ir IS administratoriaus įgaliojimus, teises, pareigas, jų supažindinimo su Tarnybos IS saugos politiką įgyvendinančiais dokumentais (toliau – Saugos dokumentai) tvarką ir saugaus tvarkomų duomenų teikimo IS naudotojams kontrolės tvarką.

2. Taisyklėse vartojamos sąvokos apibrėžtos 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“.

3. Taisyklės taikomos visiems IS naudotojams ir IS administratoriui (toliau visi kartu – Naudotojai).

4. Naudotojai turi turėti tik tiek prieigos prie duomenų teisių, kiek yra būtina jų tiesioginei veiklai vykdyti.

5. Prieiga prie IS Naudotojams suteikiama vadovaujantis principu „*būtina žinoti*“.

II SKYRIUS
NAUDOTOJŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

6. Naudotojai turi teisę tvarkyti elektroninę informaciją tik atlikdami savo tiesiogines funkcijas.

7. Naudotojams draudžiama savavališkai tvarkyti IS elektroninę informaciją.

8. IS administratoriui suteikiama teisė:

8.1. paskirstyti ir tvarkyti fizinę duomenų saugojimo erdvę;

8.2. organizuoti ir atlikti duomenų bazės atkūrimo darbus;

8.3. diegti naujas duomenų bazės valdymo sistemų versijas;

8.4. stebėti prieinamumą;

8.5. atlikti duomenų kopijavimo darbus;

8.6. prižiūrėti keitimosi duomenimis infrastruktūrą;

8.7. atlikti ypatingos svarbos duomenų pakeitimus;

8.8. administruoti tarnybines stotis;

8.9. administruoti IS naudotojų kompiuterizuotas darbo vietas.

9. Naudotojai vykdo IS saugos įgaliotinio nurodymus ir pavedimus, susijusius su elektroninės informacijos saugos užtikrinimu.

10. IS naudotojams suteikiama teisė:

10.1. įvesti, keisti, atnaujinti, naikinti duomenis, susijusius su jų atliekamomis funkcijomis;

10.2. atlikti duomenų paiešką ir peržiūrą.

11. Naudotojai privalo laikytis Saugos dokumentuose ir kituose teisės aktuose nustatytų reikalavimų.

12. Naudotojai privalo užtikrinti IS duomenų saugumą.

III SKYRIUS
NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS TVARKA

13. Naudotojai su Saugos dokumentais supažindinami pasirašytinai.

14. Naudotojus su Saugos dokumentais supažindina IS saugos įgaliotinis. Naudotojų susipažinimo su Saugos dokumentais sąrašus saugo IS saugos įgaliotinis.

15. Naudotojai pakartotinai su Saugos dokumentais supažindinami tik šiems dokumentams iš esmės pasikeitus.

IV SKYRIUS
SAUGAUS DUOMENŲ TEIKIMO NAUDOTOJAMS KONTROLĖS TVARKA

16. Naudotojų įregistravimo ir išregistravimo tvarka:

16.1. IS naudotojus įregistruoja ir išregistruoja IS administratorius.

16.2. IS naudotojai įregistruojami ir išregistruojami remiantis atitinkamo Tarnybos struktūrinio padalinio vadovo tarnybiniu pranešimu.

16.3. IS administratorius, jungdamasis prie duomenų bazių, papildomai tapatybę patvirtina naudodamas IS naudotojo vardą ir slaptažodį. IS administratoriui suteikiamas nesikartojantis IS naudotojo vardas ir laikinas slaptažodis. IS administratoriui suteiktas IS naudotojo vardas nekeičiamas ir negali būti suteiktas kitam IS naudotojui.

16.4. IS naudotojai turi būti autentifikuojami Valstybės informacinių išteklių sąveikumo platformos (VIISP) autentifikavimo priemonėmis arba naudoti suteiktą IS naudotojo vardą. Naudoti svetimą IS naudotojo vardą griežtai draudžiama.

17. Reikalavimai slaptažodžių sudarymui, galiojimo trukmei, keitimui ir saugojimui:

17.1. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais. IS saugos įgaliotinio sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jei:

17.1.1. IS naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio;

17.1.2. nėra techninių galimybių IS naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu.

17.2. Suteiktas laikinas slaptažodis turi būti pakeistas pirmojo prisijungimo prie metu.

17.3. IS naudotojo slaptažodį turi sudaryti ne mažiau kaip 8 simboliai, IS administratoriaus – ne mažiau kaip 12 simbolių.

17.4. Slaptažodis turi būti sudarytas iš raidžių, skaitmenų ir specialiųjų simbolių.

17.5. Slaptažodžiui sudaryti patartina nenaudoti asmeninės informacijos (pavyzdžiui, savo ar vaiko gimimo datos, gyvenamosios vietos adreso sudėtinių dalių, namo, buto numerio, vaikų vardų ir panašiai), nesudaryti iš žodynuose pateikiamų žodžių, nenaudoti iš eilės einančių skaičių ar raidžių.

17.6. IS naudotojo slaptažodis turi būti keičiamas ne rečiau kaip kas 90 dienų, IS administratoriaus – ne rečiau kaip kas 60 dienų.

17.7. Draudžiama naudoti tą patį slaptažodį darbo ir nedarbinei veiklai.

17.8. Slaptažodis turi būti įsimenamas, draudžiama slaptažodį užsirašyti ar atskleisti kitam asmeniui.

17.9. Kilus įtarimų, kad slaptažodis galėjo būti atskleistas, Naudotojas turi nedelsdamas slaptažodį pakeisti.

17.10. Pasirinkdamas ar keisdamas slaptažodį, Naudotojas turi bent kartą slaptažodį pakartoti.

17.11. Keičiant IS naudotojo slaptažodį, neturi būti leidžiama sudaryti slaptažodžio iš buvusių 6 paskutinių slaptažodžių, IS administratoriaus – iš buvusių 3 paskutinių slaptažodžių.

17.12. Slaptažodžiai turi būti saugomi naudojant maišos funkcijas.

17.13. IS dalys, atliekančios nuotolinio prisijungimo autentikavimą, turi neleisti automatiškai išsaugoti slaptažodžius.

18. Didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius – 5 kartai. Neteisingai įvedus slaptažodį didžiausią leistiną mėginimų skaičių, IS užsirakina ir neleidžia Naudotojui identifikuotis 15 minučių.

19. Naudotojams prieigos teisės dirbti su IS gali būti suteiktos tik pasirašius pasižadėjimą saugoti tvarkomų duomenų paslaptį, laikytis duomenų saugos reikalavimų ir pasirašytinai susipažinus su Saugos dokumentais.

20. IS naudotojų teisės dirbti su elektronine informacija ribojimas ir naikinimas:

20.1. Iš darbo atleidžiamo IS naudotojo struktūrinio padalinio vadovas arba jo įgaliotas asmuo elektroniniu laišku informuoja IS administratorių apie prieigos teisių dirbti su elektronine informacija panaikinimą ne vėliau kaip paskutinę IS naudotojo darbo Tarnyboje dieną. Atleistų Tarnybos darbuotojų IS naudotojo registracijos duomenys nedelsiant blokuojami.

20.2. Keičiantis darbuotojo pareiginėms funkcijoms, turi būti peržiūrimos jo prieigos prie IS teisės.

21. Nuotoliniam prisijungimui prie IS taikomi reikalavimai:

21.1. Visi nuotoliniai prisijungimai prie IS turi būti šifruojami ir fiksuojami kontrolės žurnale.

21.2. Leidimą IS naudotojams prisijungti nuotoliniu būdu prie IS duoda Tarnybos direktorius ar jo įgaliotas asmuo.

21.3. IS naudotojams nuotolinę prieigą prie IS suteikia IS administratorius, gavęs Tarnybos direktoriaus ar jo įgalioto asmens raštišką leidimą.

21.4. Kiti reikalavimai yra nustatyti Lietuvos Respublikos ryšių reguliavimo tarnybos kompiuterių tinklo, kompiuterinės ir programinės įrangos naudojimo ir administravimo tvarkos apraše, patvirtintame Tarnybos direktoriaus 2018 m. spalio 2 d. įsakymu Nr. 1V-921 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos kompiuterių tinklo, kompiuterinės ir programinės įrangos naudojimo ir administravimo tvarkos aprašo patvirtinimo“.

Pakeitimai:

1.
Lietuvos Respublikos ryšių reguliavimo tarnyba, Įsakymas
Nr. (1.9E)1V-51, 2021-01-13, paskelbta TAR 2021-01-19, i. k. 2021-00851
Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos direktoriaus 2019 m. vasario 26 d. įsakymo Nr. 1V-240 „Dėl Lietuvos Respublikos ryšių reguliavimo tarnybos informacinių sistemų saugos dokumentų patvirtinimo“ pakeitimo