Suvestinė redakcija nuo 2023-07-29

Įsakymas paskelbtas: TAR 2021-04-09, i. k. 2021-07516

SVEIKATOS APSAUGOS MINISTERIJOS
EKSTREMALIŲ SVEIKATAI SITUACIJŲ CENTRO
DIREKTORIUS

ĮSAKYMAS
DĖL EKSTREMALIŲ SITUACIJŲ VALDYMO INFORMACINĖS SISTEMOS NUOSTATŲ IR EKSTREMALIŲ SITUACIJŲ VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATŲ PATVIRTINIMO

2021 m. balandžio 8 d. Nr. 05-36
Kaunas

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 8 straipsnio 3 dalimi, 30 straipsniu, Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“4 ir 11 punktais ir 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, 19 ir 26 punktais:

1. Į s t e i g i u Ekstremalių situacijų valdymo informacinę sistemą.

2. T v i r t i n u pridedamus:

2.1. Ekstremalių situacijų valdymo informacinės sistemos nuostatus;

2.2. Ekstremalių situacijų valdymo informacinės sistemos duomenų saugos nuostatus;

3. P a v e d u Ekstremalių situacijų valdymo informacinės sistemos pagrindiniam tvarkytojui:

3.1. paskirti Ekstremalių situacijų valdymo informacinės sistemos saugos įgaliotinį, administratorių, duomenų valdymo įgaliotinį;

3.2. per 30 kalendorinių dienų nuo šio įsakymo įsigaliojimo parengti ir teisės aktų nustatyta tvarka suderinti bei Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centrui pateikti tvirtinti:

3.2.1. Ekstremalių situacijų valdymo informacinės sistemos naudotojų administravimo taisyklių projektą;

3.2.2. Ekstremalių situacijų valdymo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių projektą;

3.2.3. Ekstremalių situacijų valdymo informacinės sistemos veiklos tęstinumo valdymo plano projektą.

Direktorius Olegas Sitnikovas

SUDERINTA :
dėl informacinės sistemos nuostatų:

Lietuvos Respublikos sveikatos apsaugos ministerijos 2021-03-25 raštu Nr. 10-1987

Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos 2021-03-25 raštu Nr.S-122(2021)

Nacionalinio visuomenės sveikatos centro prie Sveikatos apsaugos ministerijos 2021-04-01 raštu Nr. (06 1.9 Mr)2-53661

Valstybinės duomenų apsaugos inspekcijos 2021-03-30 raštu Nr. 2R-1507 (3.2.Mr)

Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos 2021-03-26 raštu (14.59E) I-2083

Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos 2021-03-24 raštu Nr. (4.1 E) 6K-223

Nacionalinės švietimo agentūros 2021-03-25 raštu Nr.SD-682(1.6 E)

Lietuvos Respublikos ekonomikos ir inovacijų ministerijos 2021-03-29 raštu Nr. 3-1450

SUDERINTA:
dėl saugos nuostatų:
Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos 2021-04-08 raštu Nr. (4.1 E) 6K-283

VšĮ Kauno miesto greitosios medicinos pagalbos stoties 2021-04-08 raštu Nr.SAS-11 (1.6)

PATVIRTINTA
Sveikatos apsaugos ministerijos
Ekstremalių sveikatai situacijų centro
direktoriaus pavaduotoja, pavaduojanti
direktorių 2023 m. liepos 28 d.
įsakymu Nr. V-87

EKSTREMALIŲ SITUACIJŲ VALDYMO INFORMACINĖS SISTEMOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Ekstremalių situacijų valdymo informacinės sistemos nuostatai (toliau – Nuostatai) nustato Ekstremalių situacijų valdymo informacinės sistemos (toliau – ESVIS, Informacinė sistema) steigimo teisinį pagrindą, tikslus, uždavinius, pagrindines funkcijas, organizacinę, informacinę ir funkcinę struktūras, duomenų naudojimo, teikimo, saugos, finansavimo, modernizavimo ir likvidavimo tvarką.

2. Informacinės sistemos steigimo ir naujų jos funkcijų diegimo teisinis pagrindas yra Lietuvos Respublikos sveikatos sistemos įstatymo Nr. I-552 2 straipsnio pakeitimo ir įstatymo papildymo 12^1 ir 51^1 straipsniais įstatymas, Pacientų pavėžėjimo paslaugos teikimo taisyklės, patvirtintos Lietuvos Respublikos sveikatos apsaugos ministro 2023 m. sausio 23 d. įsakymu Nr. V-90 „Dėl Pacientų pavėžėjimo paslaugos teikimo taisyklių patvirtinimo", Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro nuostatų, patvirtintų Lietuvos Respublikos sveikatos apsaugos ministro 2008 m. gruodžio 9 d. įsakymu Nr. V-1246 „Dėl Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro nuostatų patvirtinimo" 10.1., 11.3., 11.4. papunkčiai.

3. ESVIS tvarkoma vadovaujantis šiais teisės aktais:

3.1. Lietuvos Respublikos civilinis kodeksas;

3.2. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

3.3. Lietuvos Respublikos sveikatos sistemos įstatymas;

3.4. Lietuvos Respublikos teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatymas;

3.5. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

3.6. Lietuvos Respublikos kibernetinio saugumo įstatymas;

3.7. 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) (toliau – Reglamentas (ES) 2016/679);

3.8. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo (toliau kartu – Bendrųjų elektroninės informacijos saugos ir kitų informacinių sistemų gairių aprašas);

3.9. Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo" (toliau – Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas);

3.10. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

3.11. Pacientų pavėžėjimo paslaugų organizavimo ir teikimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2022 m. lapkričio 30 d. nutarimu Nr. 1196 „Dėl Pacientų pavėžėjimo paslaugų organizavimo ir teikimo tvarkos aprašo patvirtinimo”;

3.12. Lietuvos Respublikos Vyriausybės 2010 m. kovo 17 d. nutarimas Nr. 286 “Dėl Lietuvos Respublikos civilinės saugos įstatymo, Lietuvos Respublikos visuomenės sveikatos priežiūros įstatymo, Lietuvos Respublikos socialinių paslaugų įstatymo atitinkamų nuostatų įgyvendinimo”;

3.13. Minimalaus savivaldybėse užtikrinamų asmens sveikatos priežiūros paslaugų, dėl kurių gavimo ir/ar grįžimui gavus jas vykdomas savivaldybės lygmens pacientų pavėžėjimo paslaugų teikimas, sąrašas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2023 m. sausio 11 d. įsakymu Nr. V-32 „Dėl Minimalaus savivaldybėse užtikrinamų asmens sveikatos priežiūros paslaugų, dėl kurių gavimo ir/ar grįžimui gavus jas vykdomas savivaldybės lygmens pacientų pavėžėjimo paslaugų teikimas, sąrašo patvirtinimo“;

3.14. Pacientų pavėžėjimo paslaugų teikimo stebėsenos tvarkos aprašas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2023 m. sausio 11 d. įsakymu Nr. V-33 „Dėl Pacientų pavėžėjimo paslaugų teikimo stebėsenos tvarkos aprašo patvirtinimo“;

3.15. Specializuoto pacientų pavėžėjimo paslaugų teikimo tvarkos aprašas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2023 m. sausio 11 d. įsakymu Nr. V-34 „Dėl Specializuoto pacientų pavėžėjimo paslaugų teikimo tvarkos aprašo patvirtinimo“;

3.16. Pacientų pavėžėjimo paslaugos teikimo taisyklės, patvirtintos Lietuvos Respublikos sveikatos apsaugos ministro 2023 m. sausio 23 d. įsakymu Nr. V-90 „Dėl Pacientų pavėžėjimo paslaugos teikimo taisyklių patvirtinimo“;

3.17. Valstybės ir savivaldybių institucijų ir įstaigų, ūkio subjektų ir kitų įstaigų, savivaldybių administracijų kaupiamų asmeninės apsaugos priemonių ir kitų veiklos vykdymui užtikrinti būtinų priemonių, skirtų apsisaugoti nuo pavojingos ar ypač pavojingos užkrečiamosios ligos, atsargų sąrašas bei šių priemonių kiekio apskaičiavimo tvarkos aprašas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2021 m. sausio 27 d įsakymu Nr. V-160 „Dėl Valstybės ir savivaldybių institucijų ir įstaigų, ūkio subjektų ir kitų įstaigų, savivaldybių administracijų kaupiamų asmeninės apsaugos priemonių ir kitų veiklos vykdymui užtikrinti būtinų priemonių, skirtų apsisaugoti nuo pavojingos ar ypač pavojingos užkrečiamos ligos atsargų sąrašo bei šių priemonių kiekio apskaičiavimo tvarkos aprašo patvirtinimo“;

3.18. Sveikatos priežiūros sistemos subjektuose kaupiamų asmeninės apsaugos priemonių ir kitų veiklos vykdymui užtikrinti būtinų priemonių, skirtų pasirengti ekstremaliųjų situacijų, sukeltų cheminių, biologinių veiksnių, branduolinių ar radiologinių avarijų bei teroristinių išpuolių likvidavimui ir jų padarinių šalinimui, atsargų sąrašų ir šių priemonių minimalaus sukauptino kiekio (normatyvų) bei kaupimo terminų tvarkos aprašas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2021 m. spalio 4 d. įsakymu Nr. V-2225 „Dėl Sveikatos priežiūros sistemos subjektuose kaupiamų asmeninės apsaugos priemonių ir kitų veiklos vykdymui užtikrinti būtinų priemonių, skirtų pasirengti ekstremaliųjų situacijų, sukeltų cheminių, biologinių veiksnių, branduolinių ar radiologinių avarijų bei teroristinių išpuolių likvidavimui ir jų padarinių šalinimui, atsargų sąrašų ir šių priemonių minimalaus sukauptino kiekio (normatyvų) bei kaupimo terminų tvarkos aprašo patvirtinimo“;

3.19. Sveikatos apsaugos ministerijos 2021–2023 m. ekstremaliųjų situacijų prevencijos priemonių planas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2020 m. gruodžio 30 d. įsakymu Nr. V-3061 ”Dėl Sveikatos apsaugos ministerijos 2021–2023 metų ekstremaliųjų situacijų prevencijos priemonių plano patvirtinimo”;

3.20. Visuomenės sveikatos priežiūros įstaigos ekstremaliųjų situacijų valdymo plano rengimo rekomendacijos, patvirtintos Lietuvos Respublikos sveikatos apsaugos ministro 2019 m. balandžio 23 d. įsakymu Nr. V-455 „Dėl visuomenės sveikatos priežiūros įstaigos ekstremaliųjų situacijų valdymo plano rengimo rekomendacijų patvirtinimo“;

3.21. Informacijos apie sveikatos priežiūros įstaigų pasirengimą veiklai ekstremaliųjų situacijų atvejais teikimo tvarkos aprašas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2011 m. gruodžio 23 d. įsakymu Nr. V-1110 „Dėl Informacijos apie sveikatos priežiūros įstaigų pasirengimą veiklai ekstremaliųjų situacijų atvejais teikimo tvarkos aprašo patvirtinimo“;

3.22. Keitimosi informacija apie ekstremaliąsias situacijas, ekstremaliuosius įvykius ir kitus riziką gyventojų sveikatai ir gyvybei keliančius įvykius tvarkos aprašas, patvirtintas Lietuvos Respublikos sveikatos apsaugos ministro 2010 m. liepos 23 d. įsakymu Nr. V-657 “Dėl Keitimosi informacija apie ekstremaliąsias situacijas, ekstremaliuosius įvykius ir kitus riziką gyventojų sveikatai ir gyvybei keliančius įvykius tvarkos aprašo patvirtinimo“;

3.23. Būtinųjų priešnuodžių rinkinio asmens sveikatos priežiūros įstaigose įsigijimo ir priešnuodžių vartojimo tvarkos aprašas ir Priešnuodžių, vartojamų apsinuodijusiems pacientams gydyti asmens sveikatos priežiūros įstaigose, sąrašas, patvirtinti Lietuvos Respublikos sveikatos apsaugos ministro 2004 m. birželio 28 d. įsakymu Nr. V-468 „Dėl Būtinųjų priešnuodžių rinkinio asmens sveikatos priežiūros įstaigose įsigijimo ir vartojimo tvarkos ir Priešnuodžių, vartojamų apsinuodijusiems pacientams gydyti asmens sveikatos priežiūros įstaigose, sąrašo patvirtinimo“;

3.24. Asmens sveikatos priežiūros įstaigos ekstremaliųjų situacijų valdymo plano rengimo rekomendacijos, patvirtintos Lietuvos Respublikos sveikatos apsaugos ministro 2003 m. kovo 6 d. įsakymu Nr. V-157 „Dėl Asmens sveikatos priežiūros įstaigos ekstremaliųjų situacijų valdymo plano rengimo rekomendacijų patvirtinimo”;

3.25. Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro Lietuvos nacionalinės sveikatos sistemos įstaigų parengties ekstremaliosioms situacijoms stebėsenos procesų dokumentacija, patvirtinta Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro direktoriaus 2022 m. gruodžio 30 d. įsakymu Nr. V-110 „Dėl sveikatos apsaugos ministerijos ekstremalių sveikatai situacijų centro Lietuvos nacionalinės sveikatos sistemos įstaigų parengties ekstremaliosioms situacijoms stebėsenos procesų dokumentacijos patvirtinimo“;

3.26. Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro nuostatai, patvirtinti Lietuvos Respublikos sveikatos apsaugos ministro 2008 m. gruodžio 9 d. įsakymu Nr. V-1246 “Dėl Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro nuostatų patvirtinimo”;

3.27. Ūkio subjekto, kitos įstaigos ekstremaliųjų situacijų valdymo plano rengimo metodinės rekomendacijos ir Ministerijos, kitos valstybės institucijos ir įstaigos ekstremaliųjų situacijų valdymo plano rengimo metodinės rekomendacijos, patvirtintos Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2011 m. vasario 23 d. įsakymu Nr. 1-70 „Dėl Ekstremaliųjų situacijų valdymo planų rengimo metodinių rekomendacijų patvirtinimo“;

3.28. Ūkio subjekto, kitos įstaigos galimų pavojų ir ekstremaliųjų situacijų rizikos analizės metodinės rekomendacijos ir Ministerijos, kitos valstybės institucijos ir įstaigos galimų pavojų ir ekstremaliųjų situacijų rizikos analizės metodinės rekomendacijos, patvirtintos Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2011 m. birželio 2 d. įsakymu Nr. 1-189 „Dėl Galimų pavojų ir ekstremaliųjų situacijų rizikos analizės atlikimo rekomendacijų patvirtinimo“;

3.29. Kriterijai ūkio subjektams ir kitoms įstaigoms, kurių vadovai turi organizuoti ekstremaliųjų situacijų valdymo planų rengimą, derinimą ir tvirtinimą, ir ūkio subjektams, kurių vadovai turi sudaryti ekstremaliųjų situacijų operacijų centrą, patvirtini Priešgaisrinės apsaugos ir gelbėjimo departamento prie Vidaus reikalų ministerijos direktoriaus 2010 m. balandžio 19 d. įsakymu Nr. 1-134 „Dėl Kriterijų ūkio subjektams ir kitoms įstaigoms, kurių vadovai turi organizuoti ekstremaliųjų situacijų valdymo planų rengimą, derinimą ir tvirtinimą, ir ūkio subjektams, kurių vadovai turi sudaryti ekstremaliųjų situacijų operacijų centrą, patvirtinimo“;

3.30. Valstybės informacinių sistemų gyvavimo ciklo valdymo metodika, patvirtinta Informacinės visuomenės plėtros komiteto prie Susisiekimo ministerijos direktoriaus 2014 m. vasario 25 d. įsakymo Nr. T-29 „Dėl Valstybės informacinių sistemų gyvavimo ciklo valdymo metodikos patvirtinimo“;

3.31. kiti teisės aktai, reglamentuojantys saugų elektroninės informacijos tvarkymą, saugojimą bei sunaikinimą.

4. Nuostatuose vartojamos sąvokos atitinka sąvokas, apibrėžtas Nuostatų 3 punkte nurodytuose teisės aktuose.

5. ESVIS tikslai yra:

5.1. informacinių technologijų priemonėmis tvarkyti Informacinėje sistemoje kaupiamus duomenis, valdyti pacientų registracijų tyrimams ir vakcinacijai veiklos procesus;

5.2. informacinių technologijų priemonėmis organizuoti paciento pavėžėjimo į (arba iš) Lietuvos nacionalinės sveikatos sistemos (toliau – LNSS) asmens sveikatos priežiūros įstaigą, kai pacientui nereikalinga skubioji medicinos pagalba, paslaugų teikimą ir administravimą, valdyti pacientų pavėžėjimo veiklos procesus;

5.3. informacinių technologijų priemonėmis užtikrinti LNSS subjektų parengtį ekstremalioms situacijoms bei koordinuoti parengties ir prevencijos veiksmus sveikatos sistemoje, valdyti parengties ekstremaliosioms situacijoms veiklos procesus.

6. ESVIS uždaviniai:

6.1. informacinių technologijų priemonėmis centralizuotai valdyti asmenų, besikreipiančių trumpuoju telefono numeriu 1808 srautus;

6.2. informacinių technologijų priemonėmis valdyti registracijas tyrimams ir vakcinacijai į SPĮ, kaupti duomenis apie registraciją ir tyrimus, jų atsakymus bei užtikrinti savalaikį informacijos ir dokumentų pateikimą ESVIS pacientams ir naudotojams;

6.3. informacinių technologijų pagalba administruoti pavėžėjimo paslaugai besiregistruojančius asmenis bei valdyti pavėžėjimo paslaugos teikimą;

6.4. informacinių technologijų priemonėmis užtikrinti parengties ir prevencijos ir stebėsenos funkcijas, taip pat koordinavimo funkcijas, sudarant sąlygas LNSS subjektams rengti ekstremalių situacijų valdymo planus informacinėje sistemoje bei ESSC vertinti SPĮ parengtį ekstremalioms situacijoms;

6.5. kaupti sisteminti ir analizuoti sveikatos sistemos įstaigų resursų, reikalingų užtikrinti jų parengtį ekstremaliosioms situacijoms, duomenis;

6.6. sudaryti sąlygas informacinių technologijų priemonėmis valdyti kompetencijų ugdymo ekstremalių sveikatai situacijų valdymo srityje procesus.

7. ESVIS pagrindinės funkcijos:

7.1. 1808 pagalbos skambučių ir SPĮ valdymo funkcijos:

7.1.1. identifikuoti besikreipiančius asmenis trumpuoju telefono numeriu 1808;

7.2. registracijos į SPĮ bei duomenų kaupimo, apdorojimo ir pateikimo ESVIS pacientams ir naudotojams funkcijos:

7.2.1. registruoti asmenis tyrimams bei sudaryti sąlygas registruotis internetu patiems ar (ir) kitose SPĮ;

7.2.2. užtikrinti savalaikį elektroninių (E200) formų kūrimą ir perdavimą į Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinę sistemą (toliau – ESPBI IS);

7.2.3. užtikrinti savalaikį atsakymų (E200-ats) apie atliktus tyrimus registravimą ir perdavimą į ESPBI IS;

7.2.4. užtikrinti atsakymų apie atliktus tyrimus bei dokumentų patvirtinančių vakcinacijos, persirgimo COVID – 19 liga (koronaviruso infekcija) ar neigiamo tyrimų rezultato faktą pateikimą pacientams;

7.3. vykdyti ESVIS sukauptos informacijos analizę, statistikos skaičiavimą, analizuoti informaciją;

7.4. kaupti elektroninę informaciją apie asmenų, besikreipiančių trumpuoju telefono numeriu 1808, registraciją tyrimams ir vakcinacijai bei pacientų pavėžėjimui, tyrimų ir vakcinacijos bei pavėžėjimo duomenų valdymą ir informavimą trumposiomis žinutėmis;

7.5. valdyti vakcinacijos procesą skiepijimo vietoje, dokumentuoti vakcinacijos faktą ir perduoti informaciją į ESPBI IS;

7.6. Pacientų pavėžėjimo paslaugos valdymas:

7.6.1. užtikrinti savarankišką registraciją pavėžėjimo paslaugai bei valdyti registraciją pavėžėjimo paslaugai gauti;

7.6.2. administruoti pavėžėjimo ir palydėjimo rezervacijas, automobilių paskyrimus, informuoti apie atliktas rezervacijas, valdyti vairuotojų maršrutus;

7.6.3. administruoti pavėžėjimo ir palydėjimo rezervacijas, automobilių paskyrimus, „palydėtojų“ paskyrimus, informuoti apie atliktas rezervacijas, valdyti vairuotojų maršrutus;

7.6.4. užtikrinti operatyvų informacijos pateikimą pavėžėjimo ir palydėjimo paslaugas teikiantiems subjektams bei pacientams ir kitoms suinteresuotoms institucijoms;

7.7. Parengties ir prevencijos valdymas:

7.7.1. sudaryti sąlygas informacinių technologijų priemonėmis rengti ekstremalių situacijų planus, koordinuoti parengtį ekstremalioms situacijoms įstaigose bei sveikatos sistemoje;

7.7.2. saugoti, analizuoti ir vertinti įstaigų parengties informaciją;

7.7.3. užtikrinti efektyvų ir į sisteminį tobulinimą orientuotą parengties stebėsenos procesą;

7.7.4. sukurti lanksčias, lengvai pritaikomas elektroninių paslaugų teikimo formas ir sisteminius procesus bei duomenų analizės priemones, suteikiančias galimybę kurti apibendrinančias ataskaitas ir realiu laiku analizuoti kaupiamus duomenis;

7.7.5. analizuoti parengties ekstremalioms sveikatai tendencijas;

7.8. Kompetencijų ekstremalių situacijų valdyme ugdymo valdymas:

7.8.1. standartizuoti ir sudaryti sąlygas valdyti, kontroliuoti ir administruoti kompetencijų, būtinų ekstremalių situacijų valdymui, ugdymo procesą;

7.8.2. užtikrinti kompetencijų ugdymo priemonių pasiekiamumą;

7.8.3. kaupti sisteminti ir analizuoti kompetencijų ugdymo proceso duomenis (kvalifikaciją kėlusius asmenų duomenis, kvalifikacijos tobulinimo renginių skaičius, ugdymosi efektyvumo ir žinių gavimo lygis bei pan.) ekstremaliųjų situacijų valdymo srityje.

8. ESVIS pacientų ir naudotojų asmens duomenų tvarkymo tikslas:

8.1. Pavėžėjimo paslaugų teikimui Paciento nuvežimo į Lietuvos nacionalinės sveikatos sistemos asmens sveikatos priežiūros įstaigą ir (ar) parvežimo iš jos, taip pat paciento pervežimo tarp skirtingų Lietuvos nacionalinės sveikatos sistemos asmens sveikatos priežiūros įstaigų, kai pacientui nereikalinga skubioji medicinos pagalba;

8.2. Pacientų ir naudotojų identifikavimo, pacientų registracijos laboratoriniams tyrimams bei vakcinavimui atlikti;

8.3. Prevencinių priemonių sveikatos priežiūros įstaigų parengties srityje taikymo ir stebėsenos;

8.4. Sukauptų duomenų analizei ir statistikai teikti i dokumentus (išrašus).

II SKYRIUS
ESVIS ORGANIZACINĖ STRUKTŪRA

9. ESVIS organizacinę struktūrą sudaro ESVIS valdytojas, ESVIS parengties ir prevencijos modulio pagrindinis tvarkytojas, ESVIS išankstinės registracijos ir vakcinacijos (toliau – AVIR modulis) ir pacientų, kai nereikalinga skubi pagalba, pavėžėjimo (toliau – Pavėžėjimo modulis) modulių pagrindinis tvarkytojas, ESVIS tvarkytojai ir ESVIS duomenų teikėjai.

10. ESVIS valdytojas, ESVIS parengties ir prevencijos modulio pagrindinis tvarkytojas ir asmens duomenų valdytojas yra Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras (toliau – ESVIS valdytojas).

11. ESVIS valdytojas:

11.1. atlieka Valstybės informacinių išteklių valdymo įstatyme valstybės informacinės sistemos valdytojui nustatytas funkcijas, turi šiame įstatyme nurodytas teises ir pareigas;

11.2. priima sprendimus, susijusius su ESVIS techninių ir programinių priemonių kūrimu, plėtros planais, likvidavimu, modernizavimu, priežiūra, administravimu ir kontroliuoja, kaip jie vykdomi;

11.3. nagrinėja tvarkytojo pasiūlymus ir priima sprendimus dėl ESVIS duomenų mainų būdo ir formato veiklos tobulinimo;

11.4. analizuoja technines, technologines, metodines ir organizacines ESVIS tvarkymo problemas ir pagal kompetenciją priima sprendimus, kurių reikia ESVIS veiklai užtikrinti;

11.5. nagrinėja tvarkytojo pasiūlymus ir priima sprendimus dėl ESVIS duomenų mainų būdo ir formato veiklos tobulinimo;

11.6. analizuoja technines, technologines, metodines ir organizacines ESVIS tvarkymo problemas ir pagal kompetenciją priima sprendimus, kurių reikia ESVIS veiklai užtikrinti;

11.7. sudaro sutartis su ESVIS duomenų teikėjais ir duomenų gavėjais arba įgalioja sudaryti sutartis pagrindinį ESVIS tvarkytoją;

11.8. techninėmis ir organizacinėmis priemonėmis užtikrina ESVIS duomenų saugą, ESVIS tvarkomų asmens duomenų konfidencialumą, vientisumą ir prieinamumą, apsaugą nuo netyčinio arba neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų ir nuo bet kokio kito neteisėto tvarkymo, taip pat saugų duomenų perdavimą kompiuteriniais tinklais;

11.9. užtikrina, kad asmens duomenys būtų renkami nuostatuose nurodytais ir teisėtais tikslais, tvarkomi vadovaujantis Reglamentu (ES) 2016/679, Asmens duomenų teisinės apsaugos įstatymu ir kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, taip pat turi kitas teisės aktuose numatytas teises ir pareigas;

11.10. teisės aktų nustatyta tvarka teikia informaciją apie ESVIS veiklą;

11.11. užtikrina, kad valstybės informacinė sistema būtų tvarkoma vadovaujantis šiuo įstatymu, valstybės informacinės sistemos nuostatais ir kitais teisės aktais;

11.12. atlieka kitus valstybės informacinės sistemos nuostatuose ir kituose teisės aktuose nustatytus veiksmus.

12. ESVIS AVIR ir pavėžėjimo modulių pagrindinis tvarkytojas ir asmens duomenų tvarkytojas yra Greitosios medicinos pagalbos tarnyba (toliau – ESVIS pagrindinis tvarkytojas).

13. ESVIS pagrindinis tvarkytojas atlieka Valstybės informacinių išteklių valdymo įstatymo nustatytas funkcijas, turi šiame įstatyme nurodytas teises ir pareigas bei:

13.1. užtikrina, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą arba jiems būtų taikomi atitinkamais teisės aktais nustatyti konfidencialumo reikalavimai;

13.2. imasi visų priemonių, kurių reikalaujama pagal Reglamento (ES) 2016/679 32 straipsnį - techninėmis ir organizacinėmis priemonėmis užtikrina ESVIS AVIR ir pavėžėjimo modulių saugą, ESVIS tvarkomų asmens duomenų konfidencialumą, vientisumą ir prieinamumą, apsaugą nuo netyčinio arba neteisėto sunaikinimo, praradimo, pakeitimo, atskleidimo be leidimo ar neteisėtos prieigos prie jų ir nuo bet kokio kito neteisėto tvarkymo, taip pat saugų duomenų perdavimą kompiuteriniais tinklais;

13.3. atsižvelgdami į ESVIS duomenų tvarkymo pobūdį, padeda ESVIS asmens duomenų valdytojui, taikydamas tinkamas technines ir organizacines priemones, kiek tai įmanoma, įgyvendinti ESVIS asmens duomenų valdytojo prievolę atsakyti į prašymus pasinaudoti Reglamento (ES) 2016/679 III skyriuje nustatytomis duomenų subjektų teisėmis;

13.4. pagal nuostatų tvarką padeda ESVIS asmens duomenų valdytojui užtikrinti Reglamento 32–36 straipsniuose nustatytų prievolių laikymąsi, atsižvelgdamas į asmens duomenų tvarkymo pobūdį ir ESVIS asmens duomenų tvarkytojo turimą informaciją;

13.5. baigus teikti su asmens duomenų tvarkymu susijusias paslaugas, ištrina visus asmens duomenis, išskyrus atvejus, kai teisės aktuose reikalaujama asmens duomenis saugoti;

13.6. pateikia ESVIS asmens duomenų valdytojui visą informaciją, būtiną siekiant įrodyti, kad vykdomos Reglamento (ES) 2016/679) nustatytos prievolės ir sudaro sąlygas bei padeda ESVIS asmens duomenų valdytojui arba kitam ESVIS asmens duomenų valdytojo įgaliotam auditoriui atlikti auditą, įskaitant patikrinimus. Nedelsdamas informuoja ESVIS asmens duomenų valdytoją, jei, jo nuomone, nurodymas pateikti informaciją pažeidžia Reglamentą (ES) 2016/679) ar kitas duomenų apsaugos nuostatas;

13.7. ESVIS asmens duomenų tvarkytojas, nustatęs asmens duomenų saugumo pažeidimą, ne vėliau kaip per 24 valandas informuoja ESVIS asmens duomenų valdytoją apie įvykusius asmens

duomenų saugumo pažeidimus – raštu ir (ar) el. paštu pateikia pranešimą pagal Reglamento (ES) 2016/679) 33 straipsnio 3 dalies reikalavimus. Asmens duomenų saugumo pažeidimai nagrinėjami vadovaujantis 2019 m. gruodžio 18 d. direktoriaus įsakymu Nr. 05-113 dėl asmens duomenų tvarkymo, saugojimo ir šių duomenų subjektų teisių įgyvendinimo Sveikatos apsaugos ministerijos Ekstremalių situacijų centre taisyklėmis su pakeitimais direktoriaus įsakymu dėl 2020 m. rugsėjo 17 d. Nr. 05-81;

13.8. registruoja ESVIS naudotojus, vadovaudamasis ESVIS naudotojų administravimo taisyklėmis;

13.9. koordinuoja ir administruoja ESVIS duomenų tvarkymą, keitimąsi duomenimis ir jų apskaitą;

13.10. Neaptarti šiuose Nuostatuose Reglamento (ES) 2016/679) 28 straipsnio 3 dalyje numatyti reikalavimai turi būti reglamentuojami sutartimi tarp ESVIS valdytojo ir ESVIS pagrindinio tvarkytojo.

14. ESVIS tvarkytojai ir asmens duomenų tvarkytojai yra sveikatinimo įstaigos ir (arba) ESVIS valdytojo arba ESVIS pagrindinio tvarkytojo pasitelkti kiti fiziniai ar juridiniai asmenys.

15. ESVIS tvarkytojai atlieka šias funkcijas:

15.1. tvarko ESVIS duomenis Nuostatuose ir kituose ESVIS veiklą reglamentuojančiuose teisės aktuose nustatyta tvarka;

15.2. skiria darbuotojus, atsakingus už ESVIS duomenų tvarkymą, užtikrina, kad duomenys būtų teisingi, tikslūs, išsamūs;

15.3. užtikrina, kad asmens duomenis tvarkyti įgalioti asmenys būtų įsipareigoję užtikrinti konfidencialumą arba jiems būtų taikomi atitinkami konfidencialumo reikalavimai;

15.4. imasi visų priemonių, kurių reikalaujama pagal Reglamento (ES) 2016/679 32 straipsnį, užtikrina organizacinėmis, techninėmis, technologinėmis ir metodinėmis priemonėmis saugų ESVIS duomenų tvarkymą;

15.5. užtikrina ESVIS duomenų tvarkymo teisėtumą, duomenų patikimumą teisės aktų nustatyta tvarka pagal jiems suteiktus įgaliojimus;

15.6. ESVIS pagrindiniam tvarkytojui teikia pasiūlymus dėl ESVIS tobulinimo;

15.7. atsižvelgdamas į asmens duomenų tvarkymo pobūdį, asmens duomenų valdytojo nustatyta tvarka padeda asmens duomenų valdytojui, taikydamas tinkamas technines ir organizacines priemones, įvykdyti asmens duomenų valdytojo prievolę, atsakyti į prašymus, pasinaudoti Reglamento (ES) 2016/679 111 skyriuje nustatytomis duomenų subjekto teisėmis;

15.8. atlieka kitas Nuostatuose ir kituose teisės aktuose, susijusiuose su ESVIS tvarkymu, nustatytas funkcijas bei užtikrina, kad duomenys būtų tvarkomi vadovaujantis valstybės informacinės sistemos nuostatais ir kitais teisės aktais;

15.9. užtikrina, kad duomenys būtų teisingi, tikslūs, išsamūs;

15.10. Neaptarti šiuose Nuostatuose Reglamento (ES) 2016/679) 28 straipsnio 3 dalyje numatyti reikalavimai turi būti reglamentuojami sutartimi.

16. ESVIS duomenų teikėjai:

16.1. Institucijos, teikiančios duomenis iš valstybės informacinių sistemų ir (arba) registrų, įregistruotų Registrų ir valstybės informacinių sistemų registre:

16.1.1. AVIR moduliui:

16.1.1.1. Valstybės įmonė Registrų centras, teikianti Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos (valdytoja – Lietuvos Respublikos sveikatos apsaugos ministerija), Lietuvos Respublikos gyventojų registro (valdytoja – Lietuvos Respublikos teisingumo ministerija), duomenis;

16.1.1.2. Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos, teikianti Privalomojo sveikatos draudimo informacinės sistemos „Sveidra“ (toliau – SVEIDRA IS) (valdytoja – Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos) duomenis;

16.1.1.3. Informacinės visuomenės plėtros komitetas, teikiantis Valstybės informacinių išteklių sąveikumo platformos (toliau – VIISP) (valdytojas – Lietuvos Respublikos ekonomikos ir inovacijų ministerija,) duomenis;

16.1.1.4. Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos, teikianti Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos (valdytoja – Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos) ir Lietuvos Respublikos apdraustųjų valstybiniu socialiniu draudimu ir valstybinio socialinio draudimo išmokų gavėjų registro (valdytoja – Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos) duomenis;

16.1.1.5. Nacionalinė švietimo agentūra, teikianti Mokinių registro (valdytojas – Lietuvos Respublikos švietimo, mokslo ir sporto ministerija), Studentų registro (valdytojas – Lietuvos Respublikos švietimo, mokslo ir sporto ministerija) ir Pedagogų registro (valdytojas – Lietuvos Respublikos švietimo ir mokslo ministerija) duomenis;

16.1.1.6. Nacionalinis visuomenės sveikatos centras prie Sveikatos apsaugos ministerijos (toliau – NVSC) teikiantis Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos (valdytoja – Lietuvos Respublikos sveikatos apsaugos ministerija) duomenis;

16.1.2. Pavėžėjimo moduliui:

16.1.2.1. valstybės įmonė Registrų centras, teikianti Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos (valdytoja – Lietuvos Respublikos sveikatos apsaugos ministerija), Išankstinės pacientų registracijos informacinės sistemos (valdytoja – Lietuvos Respublikos sveikatos apsaugos ministerija), Lietuvos Respublikos gyventojų registro (valdytoja – Lietuvos Respublikos teisingumo ministerija), duomenis;

16.1.2.2. Neįgalumo ir darbingumo nustatymo tarnyba prie Socialinės apsaugos ir darbo ministerijos, teikianti Neįgalumo ir darbingumo nustatymo tarnybos informacinės sistemos (valdytoja – Neįgalumo ir darbingumo nustatymo tarnyba prie Socialinės apsaugos ir darbo ministerijos) duomenis;

16.1.2.3. Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos, teikianti Lietuvos Respublikos draudžiamųjų privalomuoju sveikatos draudimu registro (valdytoja – Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos), Privalomojo sveikatos draudimo informacinės sistemos „Sveidra“ (valdytoja – Valstybinė ligonių kasa prie Sveikatos apsaugos ministerijos) duomenis;

16.1.2.4. Informacinės visuomenės plėtros komitetas, teikiantis Valstybės informacinių išteklių sąveikumo platformos (valdytojas – Lietuvos Respublikos ekonomikos ir inovacijų ministerija) duomenis;

16.1.2.5. Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos, teikianti Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos (valdytoja – Valstybinio socialinio draudimo fondo valdyba prie Socialinės apsaugos ir darbo ministerijos) duomenis.

16.1.3. Parengties ir prevencijos moduliui (toliau – PP moduliui):

16.1.3.1. Higienos institutas, teikiantis Visuomenės sveikatos priežiūros specialistų registro (valdytoja – Lietuvos Respublikos sveikatos apsaugos ministerija) duomenis;

16.1.3.2. Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba prie Sveikatos apsaugos ministerijos, teikianti Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos (valdytoja – Valstybinė akreditavimo sveikatos priežiūros veiklai tarnyba prie Sveikatos apsaugos ministerijos);

16.2. institucijos, teikiančios duomenis ne iš valstybės informacinių sistemų / registrų (asmens sveikatos priežiūros įstaigos, dializių centrai, Nacionalinis transplantacijos biuras);

16.3. Juridiniai asmenys, teikiantys duomenis iš savo informacinių sistemų (pavėžėjai).

17. ESVIS naudotojai yra ESVIS valdytojo, ESVIS pagrindinio tvarkytojo ir ESVIS tvarkytojų valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis, ESVIS pagrindinio tvarkytojo pasitelktų kitų juridinių ar fizinių asmenų darbuotojai, turintys teisę naudoti ir tvarkyti ESVIS duomenis, taip pat duomenų teikėjų darbuotojai, įgalioti teikti duomenis į ESVIS.

III SKYRIUS
ESVIS INFORMACINĖ STRUKTŪRA

18. ESVIS informacinę struktūrą sudaro 16.1. papunktyje nurodytų valstybės informacinių sistemų ir registrų duomenys, reikalingų ESVIS tikslams ir uždaviniams įgyvendinti:

18.1. AVIR modulyje:

18.1.1. 1808 pagalbos skambučių valdymo duomenys:

18.1.1.1. bendrieji paciento asmens duomenys: asmens vardas (-ai), pavardė (-ės) ir asmens kodas (paciento identifikatorius išoriniam teikimui);

18.1.1.2. užregistravimo tyrimui, vakcinacijai informavimo trumposiomis žinutėmis data;

18.1.1.3. asmens, atvykstančio tyrimui, vakcinacijai, atvykimo fakto į tyrimo vietą registravimas;

18.1.1.4. tyrimo paėmimo data, tyrimo atsakymo gavimo data;

18.1.1.5. tyrimo išsiuntimo trumpąja žinute data;

18.1.1.6. Duomenys apie susirgimus pagal elektronines medicinines E200 ir E200-ats formas:

18.1.1.6.1. E200 ir E200-ats duomenų kompozicijos unikalūs identifikatoriai;

18.1.1.6.2. E200 medicininės formos pavadinimas;

18.1.1.6.3. įstaigos, suformavusios tyrimą (E200), ESVIS identifikatorius, įstaigos, suformavusios tyrimą (E200), SVEIDRA IS identifikatorius, įstaigos, suformavusios tyrimo (E200) paėmimo duomenis, pavadinimas, įstaigos, suformavusios tyrimą (E200), apskrities identifikatorius (SVEIDRA IS), įstaigos, suformavusios tyrimą (E200) savivaldybės identifikatorius (SVEIDRA IS), įstaigos, suformavusios tyrimą (E200) savivaldybės pavadinimas(SVEIDRA IS);

18.1.1.6.4. E200 duomenų sukūrimo data ir laikas;

18.1.1.6.5. E200 duomenų įvedimo užbaigtumas;

18.1.1.6.6. E200 dokumento pasirašymas;

18.1.1.6.7. E200-ats duomenų sukūrimo data ir laikas;

18.1.1.6.8. E200-ats duomenų įvedimo užbaigtumas;

18.1.1.6.9. E200-ats medicininės formos pavadinimas, įstaigos, suformavusios tyrimo atsakymą (E200-ats), ESPBI IS identifikatorius, įstaigos, suformavusios tyrimo atsakymą (E200-ats) atsakymo duomenis, pavadinimas;

18.1.1.6.10. E200-ats dokumento pasirašymas;

18.1.1.6.11. paciento identifikatorius išoriniam teikimui, asmens kodas, gimimo data (nurodoma tuomet, kai pacientai neturi asmens kodo), lytis, darbovietės ekonominės veiklos kodas;

18.1.1.6.12. paciento prisirašymo įstaigos SVEIDRA IS identifikatorius, paciento prisirašymo įstaigos apskrities identifikatorius (SVEIDRA IS), paciento prisirašymo įstaigos savivaldybės identifikatorius (ne iš Adresų registro) (SVEIDRA IS), paciento prisirašymo įstaigos savivaldybės pavadinimas (SVEIDRA IS);

18.1.1.6.13. laboratorijos naudoto metodo tyrimui pavadinimas;

18.1.1.6.14. laboratorijos tyrimo rezultato duomuo E200-ats dokumente;

18.1.1.6.15. ėminio užsakymo tirti data ir laikas;

18.1.1.6.16. paėmimo data ir laikas;

18.1.1.6.17. registracijos kodas;

18.1.1.6.18. gavimo data ir laikas;

18.1.1.6.19. tyrimo atlikimo data ir laikas;

18.1.1.6.20. laboratorinio tyrimo tipo identifikatorius;

18.1.1.7. Vakcinacijos įrašų su vakcina nuo užkrečiamosios ligos duomenys pagal elektroninę medicininę E063 formą:

18.1.1.7.1. unikalus paciento identifikatorius, paciento asmens kodas, gimimo data (nurodoma tuomet, kai pacientai neturi asmens kodo), amžius, lytis;

18.1.1.7.2. elektroninio medicinos dokumento numeris;

18.1.1.7.3. E063 užpildymo statusas;

18.1.1.7.4. E063 pasirašymo statusas, vakcinaciją atlikusios įstaigos pavadinimas ir SVEIDROS ID, vakcinaciją atlikusios įstaigos savivaldybė, paciento prisirašymo įstaiga ir jos SVEIDROS ID, paciento prisirašymo įstaigos savivaldybė;

18.1.1.7.5. vaistinio preparato nacionalinis pakuotės identifikatorius (NPAKID), vaisto prekinis pavadinimas, serijos numeris, vakcinacija / revakcinacija, pagal skiepijimo schemą kelinta vakcinos dozė įskiepyta, skiepijimo data;

18.1.1.7.6. E063 dokumento pasirašymo data;

18.1.1.8. Duomenys iš E025 formų (ambulatorinis apsilankymas), kuriose nurodyta viena iš diagnozių: Z29.0, U07.1, U07.2, U07.3 netaikant jokių kitų duomenų atrankos kriterijų – kompozicijos identifikatorius, unikalus duomenų rinkiniui, kompozicijos sukūrimo data ir baigtumo būklė, paciento identifikatorius, asmens kodas, vardas ir pavardė, įstaigos kodas ir pavadinimas, TLK-10AM klasifikacijos kodas;

18.1.2. Nacionalinės švietimo agentūros tvarkomų registrų duomenys:

18.1.2.1. Mokinių registro duomenys – mokinio, kuris mokosi pagal pradinio, pagrindinio, vidurinio ugdymo ir (ar) formaliojo profesinio mokymo, neformaliojo vaikų švietimo ir formalųjį švietimą papildančias, ikimokyklinio ir priešmokyklinio ugdymo programas, vardas pavardė, asmens kodas, švietimo teikėjo (-ų) (padalinio (-ių), kuriame (-iuose) mokosi, pavadinimas (-ai) ir juridinio asmens kodas (-ai);

18.1.2.2. Studentų registro duomenys – aukštosios mokyklos studento vardas, pavardė, asmens kodas, valstybė iš kurios atvyko, švietimo teikėjo (-ų) (padalinio (-ių), kuriame (-iuose) mokosi, pavadinimas (-ai) ir juridinio asmens kodas (-ai);

18.1.2.3. Pedagogų registro duomenys – bendrojo ugdymo mokyklos, ikimokyklinio ugdymo mokyklos, profesinio mokymo įstaigos, neformaliojo vaikų švietimo mokyklos ir formalųjį švietimą papildančio ugdymo mokyklos, mokslo ir studijų institucijų, kito švietimo teikėjo, vykdančio formaliojo ir (ar) neformaliojo švietimo programas, mokslinius tyrimus pedagogo vardas, pavardė, asmens kodas; institucijos (-ų) (padalinio (-ių)), kurioje (-iose) dirba, juridinio asmens kodas (-ai);

18.1.3. NVSC tvarkomos Užkrečiamųjų ligų, galinčių išplisti ir kelti grėsmę, stebėsenos ir kontrolės informacinės sistemos duomenys:

18.1.3.1. ligonio, asmens, įtariamo, kad serga, ir sąlytį turėjusių asmenų duomenys;

18.1.4. Valstybinio socialinio draudimo fondo valdyba teikia duomenis apie duomenų subjekto draudėją:

18.1.4.1. duomenys apie duomenų subjektą (vardas, pavardė ir asmens kodas arba gimimo data, arba socialinio draudimo numeris);

18.1.4.2. Duomenų subjekto draudėją (juridinio arba fizinio asmens kodas), užklausos laikotarpį (data „Nuo“, „Iki“), klausiančiojo juridinio asmens kodą bei tikslo kodą „X“ gauti asmens duomenis apie Duomenų subjektą: apdraustojo kategoriją („Darbuotojas“, „Nedraudiminis laikotarpis“, „Praktiką atliekantis asmuo“, „Vaiko priežiūros arba tėvystės atostogos“, „Savarankiškai dirbantis asmuo nuo 2009 metų“, „Užsienietis, turintis vizą“, „Asmuo, dirbantis pagal terminuotą darbo sutartį (VSDĮ 8 str. 2 d.)“, „Užsienietis, dirbantis pagal terminuotą darbo sutartį (VSDĮ 8 str. 2 d.)“;

18.1.5. Valstybės įmonė Registrų centras tvarkomi duomenys:

18.1.5.1. Gyventojų registro duomenys: asmens kodas, asmens gimimo data (nurodoma tuomet, kai pacientai neturi asmens kodo), asmens vardas, asmens pavardė, gyvenamoji vieta (gyvenamosios vietos savivaldybė, gyvenamosios vietos seniūnija, gyvenamosios vietos miesto / kaimo pavadinimas, gyvenamosios vietos gatvės pavadinimas, gyvenamosios vietos namo numeris, gyvenamosios vietos buto numeris), atvykimo į gyvenamąją vietą data; jeigu asmuo išvyksta gyventi į užsienį, - išvykimo vieta (valstybė) ir išvykimo data; informacija apie savivaldybę, kurioje asmuo gyvena (jei asmuo neturi deklaruotos gyvenamosios vietos);

18.1.5.2. Iš ESPB IS teikiami Nuostatų 18.1.1.3., 18.1.1.10., 18.1.1.11., 18.1.1.12. papunkčiuose nurodyti duomenys ir Nuostatų 18.1.1.13. papunktyje nurodytas dokumentas.

18.1.6. VIISP teikiami Nuostatų 18.1.1.3. papunktyje nurodyti duomenys.

18.1.7. Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos ir Lietuvos Respublikos apdraustųjų valstybiniu socialiniu draudimu ir valstybinio socialinio draudimo išmokų gavėjų registro teikiami Nuostatų 18.1.4. punkte nurodyti duomenys, reikalingus patikrinti, ar fizinis asmuo dirba pas užklausoje nurodytą draudėją.

18.2. Pavėžėjimo modulio duomenys tvarkomi ir saugomi ESVIS ir Valstybės duomenų valdymo platformos aplinkoje:

18.2.1. Elektroninės sveikatos paslaugų ir bendradarbiavimo infrastruktūros informacinės sistemos duomenys:

18.2.1.1. siuntimo duomenys (asmens kodas, siuntimo būsena, siuntimo ID, data, kada buvo išduotas siuntimas, siuntimą išdavusi asmens sveikatos priežiūros įstaiga (toliau – ASPĮ), siuntimą išdavusios ASPĮ ID, siuntimą išdavusio specialisto profesinė kvalifikacija, siuntimą išdavusio specialisto profesinės kvalifikacijos ID, specialisto, kuriam siunčiama, profesinės kvalifikacija arba skyriaus specializacija, specialisto, kuriam siunčiama, profesinės kvalifikacijos ID, pavėžėjimo tipas, pavėžėjimo pastabos);

18.2.2. Išankstinės pacientų registracijos informacinės sistemos duomenys:

18.2.2.1. išankstinės paciento registracijos duomenys (asmens kodas, registracijos būsena, data ir laikas, kada planuojamas vizitas, data ir laikas, kada planuojama vizito pabaiga, ASPĮ, kurioje vyks vizitas, pavadinimas, ASPĮ, kurioje vyks vizitas, ID, ASPĮ registratūros adresas, vizito kabineto numeris, vizito kabineto pavadinimas, ASPĮ registratūros telefono numeris, vizito paslaugos pavadinimas, vizito specialisto profesinė kvalifikacija);

18.2.3. Lietuvos Respublikos gyventojų registro duomenys:

18.2.3.1. asmens kodas (įskaitant nepilnamečių vaikų asmens kodus), lytis, asmens gimimo data (nurodoma tuomet, kai pacientai neturi asmens kodo), asmens vardas, asmens pavardė, gyvenamoji vieta (gyvenamosios vietos savivaldybė, gyvenamosios vietos seniūnija, gyvenamosios vietos miesto / kaimo pavadinimas, gyvenamosios vietos gatvės pavadinimas, gyvenamosios vietos namo numeris, gyvenamosios vietos buto numeris), informacija apie savivaldybę, kurioje asmuo gyvena (jei asmuo neturi deklaruotos gyvenamosios vietos);

18.2.4. Informacinės visuomenės plėtros komiteto tvarkomos Valstybės informacinių išteklių sąveikumo platformos fizinio asmens identifikaciniai duomenys (asmens kodas), skirti identifikuoti asmenį elektroninių paslaugų gavimo metu;

18.2.5. Valstybinio socialinio draudimo fondo valdybos prie Socialinės apsaugos ir darbo ministerijos informacinės sistemos duomenys:

18.2.5.1. asmens kodas, požymis, kad senatvės pensijos amžių sukakusiems arba Lietuvos Respublikos neįgaliųjų socialinės integracijos įstatyme nurodytiems neįgaliems asmenims, už praeitą mėnesį gautų Valstybinio socialinio draudimo fondo administravimo įstaigų mokamų socialinio draudimo pensijų, išskyrus socialinio draudimo našlių pensiją (kartu su socialinio draudimo senatvės arba netekto darbingumo (invalidumo) pensijų priemokomis), šalpos išmokų, valstybinių pensijų, užsienio valstybės pensijų, pensijų išmokų, mokamų pagal Lietuvos Respublikos pensijų kaupimo įstatymą ir Lietuvos Respublikos papildomo savanoriško pensijų kaupimo įstatymą, kompensacinių išmokų profesionaliojo scenos meno įstaigų kūrybiniams darbuotojams, valstybinių signataro rentų, valstybinių signataro našlių ir našlaičių rentų, rentų buvusiems sportininkams, kompensacijų už ypatingas darbo sąlygas ir (ar) draudžiamųjų pajamų, kaip jos apibrėžtos Lietuvos Respublikos valstybinio socialinio draudimo įstatyme, suma sudaro mažiau kaip 100 procentų einamųjų metų minimalių vartojimo poreikių dydžio, apskaičiuoto Lietuvos Respublikos socialinės paramos išmokų atskaitos rodiklių ir bazinio bausmių ir nuobaudų dydžio nustatymo įstatymo nustatyta tvarka;

18.2.6. Neįgalumo ir darbingumo nustatymo tarnybos informacinės sistemos duomenys:

18.2.6.1. asmens kodas, darbingumo lygis (proc.), darbingumo lygio nustatymo laikotarpio pradžia, darbingumo lygio nustatymo laikotarpio pabaiga, neįgalumo lygis, neįgalumo lygio nustatymo laikotarpio pradžia, neįgalumo lygio nustatymo laikotarpio pabaiga, specialiųjų poreikių

lygis, specialiųjų poreikių lygio nustatymo laikotarpio pradžia, specialiųjų poreikių lygio nustatymo laikotarpio pabaiga;

18.2.7. Lietuvos Respublikos draudžiamųjų privalomuoju sveikatos draudimu registro duomenys:

18.2.7.1. asmens kodas arba draudžiamojo identifikavimo kodas, galiojančio privalomojo sveikatos draudimo laikotarpio pradžios data, galiojančio privalomojo sveikatos draudimo laikotarpio pabaigos data;

18.2.8. Privalomojo sveikatos draudimo informacinės sistemos SVEIDRA IS duomenys:

18.2.8.1. asmens prisirašymo prie ASPĮ duomenys (asmens kodas, prisirašymo ASPĮ pavadinimas, prisirašymo ASPĮ ID, prisirašymo ASPĮ savivaldybė, prisirašymo ASPĮ savivaldybės ID, prisirašymo ASPĮ laikotarpio pradžia, prisirašymo ASPĮ laikotarpio pabaiga);

18.3. PP modulyje tvarkomi duomenys:

18.3.1. Higienos instituto tvarkomų registrų ir informacinių sistemų duomenys:

18.3.1.1. Visuomenės sveikatos priežiūros specialistų registro duomenys:

18.3.1.1.1. profesinė kvalifikacija;

18.3.1.1.2. įstaigos (-ų), kurioje (-iose) dirba Registro objektas, pavadinimas (-ai), juridinio asmens kodas (-ai), įstaigos buveinės adresas (-ai);

18.3.1.1.3. įstaigos (-ų), kurioje (-iose) dirba Registro objektas grupė (-ės) ir tipas (-ai);

18.3.1.1.4. padalinio (-ių), kuriame (-iuose) dirba Registro objektas, pavadinimas (-ai) ir adresas (-ai), jeigu jis (jie) nesutampa su įstaigos buveinės adresu;

18.3.1.1.5. pareigybės (-ių) pavadinimas, pareigybės užimtumas (-ai);

18.3.1.1.6. Registro objekto kvalifikacijos tobulinimosi poreikis, metai, norimos tobulinti kompetencijos, kompetencijų sritys;

18.3.2. Valstybinė akreditavimo sveikatos priežiūros veiklai tarnybos prie Sveikatos apsaugos ministerijos tvarkomų informacinių sistemų duomenys:

18.3.2.1. Sveikatos priežiūros įstaigų licencijavimo informacinės sistemos duomenys:

18.3.2.1.1. duomenys apie ASPĮ:

18.3.2.1.1.1. ASPĮ pavadinimas;

18.3.2.1.1.2. ASPĮ sutrumpintas pavadinimas;

18.3.2.1.1.3. ASPĮ kodas;

18.3.2.1.1.4. ASPĮ teisinė forma;

18.3.2.1.1.5. ASPĮ vadovo vardas ir pavardė;

18.3.2.1.1.6. ASPĮ buveinės adresas;

18.3.2.1.1.7. ASPĮ kontaktai (telefono ryšio numeriai, fakso numeriai, el. pašto adresai, kontaktinio asmens vardas ir pavardė);

18.3.2.1.1.8. ASPĮ veiklos adresas (-ai);

18.3.2.1.1.9. ASPĮ veiklos adreso kontaktai (telefono ryšio numeriai, fakso numeriai, el. pašto adresai, kontaktinio asmens vardas ir pavardė);

18.3.2.2. duomenys apie ASPĮ filialą (-us):

18.3.2.2.1. ASPĮ filialo (-ų) pavadinimas (-ai);

18.3.2.2.2. ASPĮ filialo kodas;

18.3.2.2.3. ASPĮ filialo (-ų) buveinės adresas (-ai);

18.3.2.2.4. ASPĮ filialo buveinės (-ių) kontaktai (telefono ryšio numeriai, fakso numeriai, el. pašto adresai, kontaktinio asmens vardas ir pavardė);

18.3.2.2.5. ASPĮ filialo (-ų) veiklos adresas (–ai);

18.3.2.2.6. ASPĮ filialo (-ų) kontaktai (telefono ryšio numeriai, fakso numeriai, el. pašto adresai, kontaktinio asmens vardas ir pavardė);

18.3.2.3. duomenys apie asmens sveikatos priežiūros paslaugas:

18.3.2.3.1. paslaugos pavadinimas;

18.3.2.3.2. asmens sveikatos priežiūros lygis;

18.3.2.3.3. asmens sveikatos priežiūros paslauga pagal vietą ir laiką;

18.3.2.3.4. paslaugos profiliai (jei yra);

18.3.2.3.5. lovų skaičius (jei reikia);

18.3.2.3.6. pacientų skaičius per dieną (jei reikia);

18.3.2.3.7. duomenys apie privalomus paslaugos teikimui medicinos prietaisus (medicinos prietaiso pavadinimas, modelis, gamintojo pavadinimas, prietaiso pagaminimo metai, serijos numeris);

18.3.2.3.8. duomenys apie ASPĮ dirbančius asmens sveikatos priežiūros specialistus (vardas, pavardė, asmeniui išduotos licencijos verstis atitinkama praktika ar kito kvalifikaciją įrodančio dokumento išdavimo data, numeris, dokumentą išdavusi institucija);

18.3.2.4. ASPĮ licencijos duomenys:

18.3.2.4.1. ASPĮ dokumentų bylos numeris;

18.3.2.4.2. ASPĮ licencijos numeris;

18.3.2.4.3. ASPĮ licencijos išdavimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.4.4. ASPĮ licencijos patikslinimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.4.5. ASPĮ licencijos galiojimo (ar jos dalies) sustabdymo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.4.6. ASPĮ licencijos galiojimo (ar jos dalies) panaikinimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.4.7. ASPĮ licencijos galiojimo (ar jos dalies) atnaujinimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.4.8. ASPĮ licencijos dublikato išdavimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.4.9. laboratorijos atestavimo pažymėjimo numeris ir išdavimo data;

18.3.2.5. duomenys apie VSPĮ:

18.3.2.5.1. VSPĮ pavadinimas;

18.3.2.5.2. VSPĮ sutrumpintas pavadinimas;

18.3.2.5.3. VSPĮ kodas;

18.3.2.5.4. VSPĮ teisinė forma;

18.3.2.5.5. VSPĮ vadovo vardas ir pavardė;

18.3.2.5.6. VSPĮ buveinės adresas;

18.3.2.5.7. VSPĮ kontaktai (telefono ryšio numeriai, fakso numeriai, el. pašto adresai, kontaktinio asmens vardas ir pavardė);

18.3.2.5.8. VSPĮ veiklos adresas (-ai);

18.3.2.5.9. VSPĮ veiklos adreso kontaktai (telefono ryšio numeriai, fakso numeriai, el. pašto adresai, kontaktinio asmens vardas ir pavardė);

18.3.2.6. Duomenys apie visuomenės sveikatos priežiūros veiklos rūšis:

18.3.2.6.1. licencijuojamos visuomenės sveikatos priežiūros veiklos rūšies pavadinimas;

18.3.2.7. VSPĮ licencijos duomenys:

18.3.2.7.1. VSPĮ dokumentų bylos numeris;

18.3.2.7.2. VSPĮ licencijos numeris;

18.3.2.7.3. VSPĮ licencijos išdavimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.7.4. VSPĮ licencijos patikslinimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.7.5. VSPĮ licencijos pakeitimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.7.6. VSPĮ licencijos galiojimo sustabdymo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.7.7. VSPĮ licencijos galiojimo panaikinimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.7.8. VSPĮ licencijos galiojimo sustabdymo panaikinimo data, VASPVT direktoriaus įsakymo data ir numeris;

18.3.2.7.9. VSPĮ licencijos dublikato išdavimo data, VASPVT direktoriaus įsakymo data ir numeris.

IV SKYRIUS
ESVIS FUNKCINĖ STRUKTŪRA

19. ESVIS funkcinę struktūrą sudaro:

19.1. 1808 pagalbos skambučių valdymo funkcijos:

19.1.1. skambučių priėmimas;

19.1.2. besikreipiančių gyventojų identifikavimas;

19.1.3. gyventojų nukreipimas ir paskirstymas į darbo vietas, pagal darbuotojų specializaciją ir esamą darbo krūvį;

19.1.4. skambučio registravimo metu gautos informacijos įvedimas;

19.1.5. gyventojų, besikreipiančių į atitinkamas įstaigas per 1808, srautų planavimo funkcija;

19.1.6. siųsti informaciją el. paštu ir (ar) trumpąja žinute apie vizito rezervacijos būseną, apsilankymo atšaukimą bei priminimą apie suplanuotus apsilankymus;

19.1.7. skambučių analizė, ataskaitų formavimas, statistikos skaičiavimas;

19.2. AVIR modulis ir portalas, kurio funkcijos:

19.2.1. identifikuoti pacientus;

19.2.2. sudaryti galimybes pacientams:

19.2.2.1. nuotoliniu būdu asmenims registruotis atlikti tyrimus mobiliuose punktuose ar karščiavimo klinikose;

19.2.2.2. nuotoliniu būdu asmenims registruotis atlikti vakcinacijai, vakcinacijos punktuose;

19.2.2.3. pasirinkti mobilius punktus, karščiavimo klinikas, vakcinavimo punktus ir matyti asmenims savarankiškai visus registracijai skirtus vizitų laikus;

19.2.2.4. užsiregistruoti tik vieną kartą konkrečiai paslaugai;

19.2.2.5. nuotoliniu būdu gauti tyrimų atliktų mobiliuose punktuose ar karščiavimo klinikose rezultatus ir skaitmeninius dokumentus patvirtinančius neigiamą tyrimų rezultatą arba šiais tyrimais patvirtintą persirgimo COVID – 19 (koronaviruso infekcija) liga faktą;

19.2.2.6. nuotoliniu būdu gauti skaitmeninius dokumentus apie mobiliuose punktuose ar karščiavimo klinikose atliktą vakcinaciją ir (ar) tyrimus;

19.2.3. Sudaryti galimybes sveikatinimo specialistams ir sveikatinimo veiklą vykdančios įstaigos darbuotojams, vykdantiems registratoriaus rolei priskirtas funkcijas:

19.2.3.1. tvirtinti ir atšaukti registraciją į mobilųjį punktą, karščiavimo kliniką ar vakcinacijos punktą, jeigu ši registracija netenkina sveikatinimo veiklą vykdančios įstaigos nustatytų reikalavimų konkrečiai paslaugai gauti;

19.2.3.2. fiksuoti asmenų atvykimą tik į savo vizitų registracijas;

19.2.3.3. matyti darbovietės paslaugų eiles, registruoti ir pašalinti asmenis iš eilės;

19.2.3.4. išduoti skaitmeninius dokumentus apie mobiliuose punktuose ar karščiavimo klinikose atliktą vakcinaciją ir (ar) tyrimus.

19.2.4. Tyrimų valdymo funkcijos:

19.2.4.1. gyventojų registravimas tyrimams mobiliuose punktuose;

19.2.4.2. tikslinių grupių prioritetų ir kvotų valdymas;

19.2.4.3. gyventojų, besiregistruojančių tyrimui, sutikimo patvirtinimo formos registravimas balsu;

19.2.4.4. automatiniu registracijos laiko perdavimas tyrimo dalyviui trumposiomis žinutėmis lietuviškais rašmenimis;

19.2.4.5. gyventojo, atvykstančio tyrimui, atvykimo fakto į tyrimo vietą registravimas;

19.2.4.6. elektroninių (E200) formų kūrimas, su formų pasirašymo elektroniniu parašu funkcionalumu ir perdavimu į ESPBI IS;

19.2.4.7. laboratorinių tyrimų duomenų gautų iš laboratorijų per ESPBI IS, registravimas;

19.2.4.8. sveikatinimo veiklą vykdančių įstaigų darbuotojų suvedamų atsakymų apie atliktus tyrimus, registravimas bei perdavimas į ESPBI IS;

19.2.4.9. automatinis gautų neigiamų tyrimų rezultatų perdavimas trumposiomis žinutėmis gyventojui, kuriam atliktas tyrimas, lietuviškais rašmenimis;

19.2.4.10. gyventojų, kuriems atliktas laboratorinis tyrimas, kurio rezultatas teigiamas, registracija gydytojo konsultacijai telefonu gyventojui, paimant duomenis iš ESPBI IS;

19.2.4.11. teigiamų testų rezultatų pacientų duomenų perdavimas į NVSC;

19.2.4.12. savivaldybių mobilių punktų bei išsidėstymo aptarnaujamoje teritorijoje stebėjimas;

19.2.4.13. apsikeitimas informacija su savivaldybių įsteigtais mobiliaisiais punktais;

19.3. Pavėžėjimo modulis, kurio funkcijos:

19.3.1. asmenų registracija pavėžėjimui;

19.3.2. asmenų patikra pavėžėjimo atitikties kriterijams;

19.3.3. asmenų informavimas apie planuojamą pavėžėjimą;

19.3.4. pavėžėjų ir palydėtojų administravimas;

19.3.5. pavėžėjų ir palydėtojų atliktų pavėžėjimų ir palydėjimų stebėjimas;

19.4. Parengties ir prevencijos modulis, kurio funkcijos:

19.4.1. užtikrinti tinkamą asmens sveikatos priežiūros įstaigų pasirengimą veiklai ekstremaliųjų situacijų atvejais;

19.4.2. užtikrinti informacijos priėmimą ir perdavimą;

19.4.3. optimizuoti ekstremalių sveikatai situacijų reagavimo procesus;

19.4.4. užtikrinti koordinavimo funkcijas;

19.4.5. rengti ekstremalių situacijų valdymo planus informacinėje sistemoje;

19.4.6. kaupti, sisteminti ir analizuoti resursus informacinėje sistemoje;

19.4.7. ESSC vertinti SPĮ parengtį ekstremalioms situacijoms;

19.4.8. rengti ataskaitas.

19.5. Kvalifikacijos tobulinimo posistemis, kurio funkcijos:

19.5.1. valdyti kompetencijų ugdymo ekstremalių sveikatai situacijų valdymo srityje procesus;

19.5.2. užtikrinti kompetencijų ugdymo priemonių pasiekiamumą;

19.5.3. kaupti, sisteminti ir vertinti informaciją apie sveikatos apsaugos sektoriaus specialistų mokymus ekstremalių situacijų valdymo srityje;

19.5.4. analizuoti kvalifikaciją kėlusių asmenų duomenis, ugdymosi efektyvumo ir žinių gavimo lygį;

19.5.5. rengti ataskaitas.

19.6. Saugios asmens sveikatos priežiūros įstaigos indekso skaičiuoklės posistemis, kurio funkcijos:

19.6.1. skaičiuoti Saugios asmens sveikatos priežiūros įstaigos indeksą;

19.6.2. vertinti SPĮ nustatytą Saugios asmens sveikatos priežiūros įstaigos indeksą;

19.6.3. užtikrinti vertinimo ir veiklų po Saugios asmens sveikatos priežiūros įstaigos indekso vertinimo rezultatų stebėseną;

19.6.4. rengti ataskaitas.

19.7. Informacinės sistemos administravimo funkcijos:

19.7.1. ESVIS naudotojų teisių suteikimas ir valdymas;

19.7.2. ESVIS naudotojų atliktų veiksmų žurnalo valdymas.

V SKYRIUS
ESVIS DUOMENŲ TEIKIMAS IR NAUDOJIMAS

20. ESVIS nuasmeninti apibendrinti duomenys yra vieši ir teikiami institucijoms, kitiems juridiniams ir fiziniams asmenims. ESVIS tvarkomi asmens duomenys teikiami ir naudojami vadovaujantis Reglamentu (ES) 2016/679, Nuostatais ir kitais asmens duomenų apsaugą reglamentuojančiais teisės aktais.

21. ESVIS apibendrinti duomenys gali būti:

21.1. pateikiami peržiūrėti leidžiamosios kreipties būdu internetu;

21.2. perduodami automatiniu būdu;

21.3. pateikiami raštu, paštu, elektroniniu paštu ar kitomis elektroninio komunikavimo priemonėmis.

22. ESVIS gavėjai gautus duomenis ir informaciją gali naudoti tik tokiam tikslui, tokios apimties ir tokiu būdu, kaip nurodyta duomenų teikimo sutartyje arba prašyme. ESVIS duomenų gavėjas negali keisti iš ESVIS gautų duomenų ir informacijos ir juos naudodamas privalo nurodyti duomenų šaltinį.

23. ESVIS duomenys Europos Sąjungos valstybių narių ir (arba) Europos ekonominės erdvės valstybių fiziniams, judriniams asmenims, juridinio statuso neturintiems subjektams, jų filialams ir atstovybėms teikiami vadovaujantis Valstybės informacinių išteklių valdymo įstatymu ir Reglamentu (ES)2016/679.

24. Kitų valstybių, išskyrus Europos Sąjungos valstybes nares ir Europos ekonominės erdvės valstybes, fiziniams, juridiniams asmenims, juridinio asmens statuso neturintiems subjektams, jų filialams ir atstovybėms duomenys teikiami, jeigu tai neprieštarauja Lietuvos Respublikos įstatymams, Reglamentui (ES) 2016/679, tarptautinėms sutartims, Europos Sąjungos teisės aktams ir kitiems norminiams teisės aktams.

25. ESVIS parengties ir prevencijos modulio duomenis teikia ESVIS parengties ir prevencijos modulio pagrindinis tvarkytojas, o ESVIS AVIR ir pavėžėjimo modulių duomenis teikia ESVIS pagrindinis tvarkytojas. Duomenys teikiami tokio turinio ir tokios formos, kokie yra naudojami ESVIS ir nereikalauja papildomo duomenų apdorojimo.

26. Daugkartinio teikimo atveju ESVIS asmens duomenys teikiami pagal ESVIS pagrindinio tvarkytojo ir duomenų gavėjo sudarytą asmens duomenų teikimo sutartį arba, kai teisės aktais yra nustatyta pareiga šiuos duomenis teikti. Sutartyje turi būti nurodyta asmens duomenų naudojimo tikslas, gavimo teisinis pagrindas, asmens duomenų naudojimo sąlygos, tvarka ir prašomų pateikti asmens duomenų apimtis.

27. Vienkartinio teikimo atveju ESVIS asmens duomenys teikiami pagal gavėjo prašymą pateiktą ESVIS pagrindiniam tvarkytojui. Prašyme turi būti nurodytas asmens duomenų naudojimo tikslas, teikimo ir gavimo teisinis pagrindas, prašomų pateikti duomenų apimtis.

28. ESVIS duomenys duomenų gavėjams teikiami neatlygintinai.

29. Kai atsisakoma teikti ESVIS tvarkomus duomenis, asmeniui, pateikusiam prašymą juos gauti, ESVIS pagrindinis tvarkytojas praneša apie priimtą sprendimą atsisakyti tenkinti asmens prašymą ir suteikia informaciją apie tokio sprendimo apskundimo tvarką.

30. Duomenų gavėjas, registro ar kitos valstybės informacinės sistemos tvarkytojas, duomenų subjektas, kiti asmenys turi teisę reikalauti ištaisyti netikslius ESVIS duomenis.

31. ESVIS pagrindinis tvarkytojas, duomenų subjekto ar institucijų, kurioms konfidencialumo reikalavimas netaikomas ir informacija gali būti suteikta tik tarnybiniais tikslais, prašymu (išreikštu rašytine forma), kuriame nurodomi pastebėti netikslumai, nedelsdamas privalo patikrinti ESVIS kaupiamus nurodytus duomenis ir, nustatęs, kad prašymas pagrįstas, ne vėliau kaip per 3 darbo dienas, ištaisyti neteisingus, neišsamius, netikslius duomenis ir (arba) sustabdyti tokių duomenų tvarkymo veiksmus, išskyrus saugojimą ir pateikti patikslintus duomenis arba motyvuotą atsisakymą juos patikslinti vadovaujantis 2019 m. gruodžio 18 d. direktoriaus įsakymu Nr. 05-113 „Dėl asmens duomenų tvarkymo, saugojimo ir šių duomenų subjektų teisių įgyvendinimo Sveikatos apsaugos ministerijos Ekstremalių situacijų centre taisyklėmis“ su pakeitimais direktoriaus įsakymu dėl 2020 m. rugsėjo 17 d. Nr. 05-81.

32. ESVIS pagrindinis tvarkytojas vadovaujantis 2021 m. gegužės 6 d. direktoriaus įsakymu Nr. 05-43 „Dėl duomenų subjektų teisių įgyvendinimo ekstremalių situacijų valdymo informacinėje sistemoje tvarkos aprašo patvirtinimo“ ne vėliau kaip per 5 darbo dienas, neatlygintinai raštu arba elektroninio ryšio priemonėmis informuoja duomenų gavėjus apie duomenų subjekto ar kito asmens prašymu ištaisytus ar sunaikintus duomenis, sustabdytus duomenų tvarkymo veiksmus, išskyrus atvejus, kai pateikti tokią informaciją būtų neįmanoma arba pernelyg sunku (dėl didelio duomenų subjektų skaičiaus, duomenų laikotarpio, nepagrįstai didelių sąnaudų). Tokiu atveju turi būti nedelsiant pranešama Valstybinei duomenų apsaugos inspekcijai.

33. Atsisakymas teikti ESVIS duomenis duomenų gavėjams gali būti skundžiamas administraciniam teismui įstatymų ir kitų teisės aktų nustatyta tvarka.

VI SKYRIUS
INFORMACINĖS SISTEMOS DUOMENŲ SAUGA

34. Informacinės sistemos duomenų saugaus tvarkymo reikalavimų įgyvendinimas užtikrinamas vadovaujantis:

34.1. Reglamento (ES) 2016/679 nustatyta tvarka;

34.2. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu;

34.3. Lietuvos standartais ir tarptautiniais standartais, reglamentuojančiais saugų informacinės sistemos duomenų tvarkymą.

35. Informacinės sistemos duomenų sauga organizuojama vadovaujantis Informacinės sistemos duomenų saugos nuostatais ir saugos politiką įgyvendinančiais dokumentais, parengtais ir patvirtintais vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo reikalavimais.

36. ESVIS naudotojai ESVIS duomenimis naudojasi pagal jiems suteiktą prieigose teisių lygmenį.

37. Informacinės sistemos naudotojai, kurie tvarko asmens duomenis, privalo pasirašyti pasižadėjimą saugoti asmens duomenų paslaptį ir neatskleisti asmens duomenų tretiesiems asmenims, jeigu šie asmens duomenys neskirti skelbti viešai. Ši pareiga galioja perėjus dirbti į kitas pareigas arba pasibaigus sutartiniams darbo ar kitiems santykiams.

38. Už ESVIS saugomų duomenų bei asmens duomenų saugą pagal kompetenciją atsako ESVIS valdytojas, ESVIS pagrindinis tvarkytojas ir tvarkytojai. Tvarkant ir saugant ESVIS kaupiamus duomenis turi būti įgyvendintos duomenų saugos organizacinės, programinės, techninės, patalpų apsaugos ir administracinės priemonės, skirtos ESVIS duomenų konfidencialumui, prieinamumui teisėtiems ESVIS tvarkytojams, vientisumui ir autentiškumui užtikrinti ir apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, naudojimo, atskleidimo, taip pat bet kokio kito neteisėto tvarkymo. Minėtos priemonės turi užtikrinti tokio lygio saugumą, kuris atitiktų saugotinų ESVIS tvarkomų duomenų pobūdį.

39. ESVIS dokumentai kaupiami ir saugomi informacinės sistemos duomenų bazėje vadovaujantis Lietuvos vyriausiojo archyvaro 2011 m. kovo 9 d. įsakymu Nr. V-100 „Dėl bendrųjų dokumentų saugojimo terminų rodyklės patvirtinimo", Pacientų pavėžėjimo paslaugos taisyklėmis, patvirtintomis Sveikatos apsaugos ministro 2023 m. sausio 23 d. įsakymu Nr. V-90 „Dėl pacientų pavėžėjimo paslaugos teikimo taisyklių patvirtinimo", Lietuvos Respublikos civilinio kodekso nuostatomis.

40. ESVIS esantys duomenys įskaitant asmens duomenis, praėjus 3 metų laikotarpiui po 1808 registracijos, po pavėžėjimo paslaugos suteikimo momento, 5 metų laikotarpiui po vakcinacijos, 25 metų laikotarpiui po laboratorinių ištyrimų, po paskutinio įrašo parengties ir prevencijos modulyje naudojami duomenys įskaitant asmens duomenis, saugomi vadovaujantis 10 metų, ištrinami iš duomenų bazės negrįžtamai arba perduodami valstybės archyvams Lietuvos Respublikos dokumentų ir archyvų įstatymo ir kitų teisės aktų nustatyta tvarka.

VII SKYRIUS
ESVIS FINANSAVIMAS

41. ESVIS kūrimas, diegimas, priežiūra ir plėtra finansuojama Lietuvos Respublikos valstybės biudžeto lėšomis bei Europos Sąjungos lėšomis.

VIII SKYRIUS
ESVIS MODERNIZAVIMAS IR LIKVIDAVIMAS

42. ESVIS modernizuojama arba likviduojama Valstybės informacinių išteklių valdymo įstatymo ir Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“ nustatyta tvarka.

43. Likviduojamos ESVIS duomenys negali būti sunaikinami, išskyrus Lietuvos Respublikos įstatymuose ar Europos Sąjungos teisės aktuose nustatytus atvejus, ir privalo būti perduodami kitai informacinei sistemai, sunaikinami arba perduodami valstybės archyvams Lietuvos Respublikos dokumentų ir archyvų įstatymo nustatyta tvarka.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

44. Duomenų subjektų teisių, įtvirtintų Reglamente (ES) 2016/679, įgyvendinimo tvarką nustato ESVIS valdytojas. Tvarka yra patvirtinta ESVIS 2019 m. gruodžio 18 d. įsakymu Nr. 05-113 „Dėl asmens duomenų tvarkymo, saugojimo ir šių duomenų subjektų teisių įgyvendinimo Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centre taisyklių patvirtinimo“ su pakeitimais 2020 m. rugsėjo 17 d. įsakymu Nr. 05-81.

45. ESVIS valdytojas ne rečiau kaip kartą per kalendorinius metus iki kiekvienų einamųjų metų pabaigos peržiūri (jei reikia tikslina ar papildo) ESVIS nuostatus, atsižvelgdama į susijusių teisės aktų ir (arba) informacinės sistemos funkcionalumų pasikeitimus.

PATVIRTINTA
Sveikatos apsaugos ministerijos
Ekstremalių sveikatai situacijų centro
direktoriaus pavaduotoja, pavaduojanti
direktorių 2023 m. liepos 28 d.
įsakymu Nr. V-87

EKSTREMALIŲ SITUACIJŲ VALDYMO INFORMACINĖS SISTEMOS DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Ekstremalių situacijų valdymo informacinės sistemos duomenų saugos nuostatai (toliau – **Saugos nuostatai**) reglamentuoja Ekstremalių situacijų informacinės sistemos (toliau – **Informacinė sistema, ESVIS**) elektroninės informacijos saugos ir kibernetinio saugumo politiką.

2. Informacinės sistemos elektroninės informacijos saugos politikos tikslas – užtikrinti Informacinės sistemos elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

3. 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 Techniniuose valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimuose, patvirtintuose 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 elektroninės informacijos saugos reikalavimai**).

4. Elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

4.1. sudaryti sąlygas saugiai automatiniu būdu tvarkyti elektroninę informaciją;

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

4.3. vykdyti elektroninės informacijos saugos (kibernetinių) incidentų, asmens duomenų saugumo pažeidimų prevenciją, reaguoti į elektroninės informacijos saugos (kibernetinius) incidentus, asmens duomenų saugumo pažeidimus ir juos operatyviai suvaldyti.

5. Informacinės sistemos elektroninės informacijos saugos užtikrinimo prioritetinės kryptys:

5.1. organizacinių, techninių, programinių, teisinių ir kitų priemonių, skirtų Informacinės sistemos elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti, įgyvendinimas ir kontrolė;

5.2. Informacinės sistemos elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

5.3. Informacinės sistemos tvarkymo kontrolė;

5.4. Informacinės sistemos paslaugų ir naudojimosi Informacinės sistemos elektronine informacija kontrolės užtikrinimas;

5.5. Informacinės sistemos tvarkomų asmens duomenų apsauga;

5.6. Informacinės sistemos veiklos tęstinumo užtikrinimas;

5.7. Informacinės sistemos naudotojų mokymas.

6. Už elektroninės informacijos saugą (kibernetinį saugumą) pagal kompetenciją atsako Informacinės sistemos valdytojas, Informacinės sistemos pagrindinis tvarkytojas ir Informacinės sistemos tvarkytojai.

7. Informacinės sistemos valdytojas atsako už elektroninės informacijos saugos (kibernetinio saugumo) politikos formavimą ir politikos įgyvendinimo organizavimą, priežiūrą ir elektroninės informacijos tvarkymo teisėtumą.

8. Informacinės sistemos pagrindinis tvarkytojas ir Informacinės sistemos tvarkytojai atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimo užtikrinimą saugos politiką įgyvendinančiuose dokumentuose (toliau – **saugos dokumentai**) nustatyta tvarka.

9. Saugos nuostatai taikomi:

9.1. Informacinės sistemos valdytojui ir pagrindiniam tvarkytojui;

9.2. kitiems Informacinės sistemos tvarkytojams;

9.3. Informacinės sistemos saugos įgaliotiniui;

9.4. Informacinės sistemos administratoriams;

9.5. Informacinės sistemos naudotojams;

9.6. Informacinei sistemai funkcionuoti reikalingų paslaugų teikėjams.

10. Informacinės sistemos valdytojo Ekstremalių svaikatai situacijų centro funkcijos:

10.1. organizuoti ir vadovauti informacinių sistemų veiklai;

10.2. rengti ir tvirtinti teisės aktus, susijusius su duomenų sauga, ir prižiūrėti, kaip jų laikomasi;

10.3. kontroliuoti, kad Informacinė sistema būtų tvarkoma vadovaujantis Lietuvos Respublikos įstatymais, Saugos nuostatais ir kitais teisės aktais;

10.4. tvirtinti Saugos nuostatus, saugos dokumentus ir kitus teisės aktus, susijusius su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu);

10.5. nagrinėti Informacinės sistemos tvarkytojų pasiūlymus dėl Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo ir priimti dėl jų sprendimus;

10.6. skirti Informacinės sistemos saugos įgaliotinį ir Informacinės sistemos administratorių;

10.7. atlikti kitas Informacinės sistemos nuostatuose ir Saugos nuostatuose nustatytas funkcijas.

11. Informacinės sistemos pagrindinio tvarkytojo funkcijos (pagal tvarkomus modulius):

11.1. atlikti Informacinės sistemos nuostatuose nustatytas funkcijas;

11.2. užtikrinti nepertraukiamą Informacinės sistemos veiklą;

11.3. užtikrinti saugų elektroninės informacijos perdavimą elektroninių ryšių tinklais;

11.4. pagal kompetenciją prižiūrėti Informacinės sistemos duomenų bazių valdymo sistemas, taikomųjų programų sistemas, ugniasienes, įsilaužimų aptikimo sistemas, elektroninės informacijos perdavimo tinklus ir kitus Informacinės sistemos komponentus, užtikrinti jų veikimą;

11.5. užtikrinti saugos dokumentų ir kitų Informacinės sistemos valdytojo priimtų teisės aktų, susijusių su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu), tinkamą įgyvendinimą;

11.6. pagal kompetenciją įgyvendinti Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus;

11.7. pagal kompetenciją užtikrinti Informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą);

11.8. teikti Informacinės sistemos valdytojui pasiūlymus dėl Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) tobulinimo;

11.9. ne rečiau kaip kartą per metus organizuoti saugos dokumentų peržiūrėjimą ir aktualizavimą;

11.10. atlikti kitas Informacinės sistemos valdytojo pavestas Informacinės sistemos nuostatuose, Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

12. Informacinės sistemos tvarkytojų funkcijos:

12.1. pagal kompetenciją prižiūrėti kompiuterius, planšetinius kompiuterius, išmaniuosius telefonus, operacines sistemas ir kitus Informacinės sistemos komponentus savo įstaigose, užtikrinti jų veikimą;

12.2. užtikrinti administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą Informacinės sistemos naudotojų kompiuteriuose ir kituose Informacinės sistemos komponentuose savo įstaigose;

12.3. užtikrinti organizacinėmis, techninėmis, technologinėmis ir metodinėmis priemonėmis saugų Informacinės sistemos elektroninės informacijos tvarkymą savo įstaigose;

12.4. valdyti elektroninės informacijos saugos (kibernetinius) incidentus savo įstaigose ir juos šalinti;

12.5. užtikrinti saugos dokumentų ir kitų Informacinės sistemos valdytojo priimtų teisės aktų, susijusių su Informacinės sistemos elektroninės informacijos sauga (kibernetiniu saugumu), tinkamą įgyvendinimą;

12.6. pagal kompetenciją įgyvendinti Informacinės sistemos elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus savo įstaigose;

12.7. pagal kompetenciją užtikrinti Informacinės sistemos elektroninės informacijos saugą (kibernetinį saugumą) savo įstaigose;

12.8. pagal kompetenciją atlikti kitas Informacinės sistemos valdytojo pavestas Informacinės sistemos nuostatuose, Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

13. Informacinės sistemos saugos įgaliotinio funkcijos:

13.1. koordinuoti ir prižiūrėti elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimą saugos dokumentuose nustatyta tvarka;

13.2. teikti Informacinės sistemos pagrindinio tvarkytojo vadovui siūlymus dėl informacinių technologijų saugos atitikties vertinimo atlikimo;

13.3. atlikti 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 – **Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas**), nustatytas asmens, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, funkcijas;

13.4. teikti Informacinės sistemos pagrindinio tvarkytojo vadovui siūlymus dėl Saugos nuostatų ir Informacinės sistemos saugos dokumentų priėmimo arba keitimo;

13.5. organizuoti Informacinės sistemos rizikos įvertinimą ir parengti rizikos įvertinimo ataskaitą;

13.6. supažindinti Informacinės sistemos administratorius ir Informacinės sistemos naudotojus su Saugos nuostatų ir saugos dokumentų reikalavimais ir atsakomybe už reikalavimų nesilaikymą;

13.7. organizuoti Informacinės sistemos naudotojų mokymus elektroninės informacijos saugos klausimais, informuoti juos apie elektroninės informacijos saugos problemas;

13.8. duoti Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Saugos nuostatų ir saugos dokumentų įgyvendinimu;

13.9. teikti Informacinės sistemos pagrindinio tvarkytojo vadovui pasiūlymus dėl koordinuojančio Informacinės sistemos administratoriaus paskyrimo ir reikalavimų jam nustatymo;

13.10. koordinuoti elektroninės informacijos saugos (kibernetinių) incidentų tyrimą savo įstaigose ir bendradarbiauti su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos (kibernetinius) incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetiniais) incidentais, išskyrus tuos atvejus, kai šią funkciją atlieka elektroninės informacijos saugos (kibernetinio saugumo) darbo grupės;

13.11. teikti Informacinės sistemos administratoriams ir Informacinės sistemos naudotojams privalomus vykdyti nurodymus ir pavedimus dėl elektroninės informacijos saugos (kibernetinio saugumo) politikos įgyvendinimo;

13.12. atlikti kitas Informacinės sistemos pagrindinio tvarkytojo vadovo pavestas Saugos nuostatuose ir saugos dokumentuose jam priskirtas funkcijas.

14. Saugos įgaliotinis negali atlikti Informacinės sistemos administratoriaus funkcijų.

15. Informacinės sistemos administratoriaus funkcijos:

15.1. užtikrinti Informacinės sistemos techninės ir programinės įrangos įdiegimą ir funkcionavimą;

15.2. diegti ir prižiūrėti programinę įrangą, reikalingą Informacinės sistemos naudotojų funkcijoms vykdyti;

15.3. suteikti teisę Informacinės sistemos naudotojams naudotis elektronine informacija, kurios reikia jų funkcijoms atlikti;

15.4. užtikrinti Informacinės sistemos komponentų (kompiuterių, tarnybinių stočių, operacinių sistemų, taikomųjų programų, duomenų bazės valdymo sistemų, ugniasienių, įsilaužimo aptikimo sistemų ir kt.) tinkamą veikimą ir priežiūrą, pagal kompetenciją nustatyti Informacinės sistemos pažeidžiamas vietas;

15.5. pagal kompetenciją dalyvauti vykdant saugumo reikalavimų įgyvendinimo stebėseną;

15.6. pagal kompetenciją teikti Informacinės sistemos pagrindinio tvarkytojo vadovui siūlymus dėl Informacinės sistemos palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir elektroninės informacijos saugos užtikrinimo;

15.7. informuoti Informacinės sistemos saugos įgaliotinį apie elektroninės informacijos saugos incidentus ir teikti siūlymus dėl elektroninės informacijos saugos incidentų pašalinimo;

15.8. daryti Informacinės sistemos duomenų bazės atsargines kopijas ir atsakyti už archyve esančių kopijų saugojimą;

15.9. atlikti kitas Informacinės sistemos pagrindinio tvarkytojo vadovo ir saugos įgaliotinio pavestas Saugos nuostatuose ir saugos dokumentuose nustatytas funkcijas.

16. Teisės aktai, kuriais vadovaujamasi tvarkant informacinių sistemų elektroninę informaciją ir užtikrinant jos saugą:

16.1. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (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);

16.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

16.3. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

16.4. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

16.5. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas;

16.6. Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašas, patvirtintas 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 – **Elektroninės informacijos svarbos nustatymo gairių aprašas**);

16.7. Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašas;

16.8. Techniniai elektroninės informacijos saugos reikalavimai;

16.9. 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“;

16.10. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Techninių

valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“ (toliau – **Informacinių technologijų saugos atitikties vertinimo metodika**);

16.11. Lietuvos ir tarptautiniai „Informacijos technologija. Saugumo metodai“ grupės standartai, nustatantys saugų elektroninės informacijos tvarkymą;

16.12. Saugos nuostatai, saugos dokumentai ir kiti teisės aktai, reglamentuojantys elektroninės informacijos saugumo politiką, jos tvarkymo teisėtumą ir saugos valdymą.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

17. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašu Informacinės sistemos tvarkoma informacija priskiriama prie svarbos informacijos kategorijos.

18. Vadovaujantis Elektroninės informacijos svarbos nustatymo gairių aprašu, Informacinė sistema priskiriama prie antrosios kategorijos.

19. Informacinės sistemos saugos įgaliotinis, atsižvelgdamas į Nacionalinio kibernetinio saugumo centro svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, kasmet organizuoja Informacinės sistemos rizikos įvertinimą. Pasikeitus Informacinės sistemos duomenų bazės struktūrai (sistemos pakeitimai, papildymas naujomis taikomosiomis programomis, taikomųjų programų pašalinimas ir kt.) ar po esminių organizacinių ar sisteminių pokyčių, nustačius naujų rizikos veiksnių, gali būti organizuojamas neeilinis Informacinės sistemos rizikos įvertinimas. Informacinės sistemos rizikos vertinimas gali būti atliekamas kartu su informacinių technologijų saugos atitikties vertinimu.

20. Organizuojant rizikos vertinimą turi būti paskirtas už rizikos vertinimo proceso priežiūrą ir tobulinimą atsakingas asmuo arba asmenys ir nustatyti jiems taikomi kvalifikaciniai reikalavimai. Atsakingu asmeniu gali būti skiriamas Informacinės sistemos pagrindinio tvarkytojo darbuotojas arba sudaroma sutartis su rizikos vertinimo, rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugas teikiančiu subjektu.

21. Informacinės sistemos rizikos vertinimo metu įvertinami rizikos veiksniai, galintys turėti įtakos Informacinės sistemos elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė, galimi rizikos valdymo būdai. Svarbiausieji rizikos veiksniai:

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

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

21.3. 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.

22. Informacinės sistemos rizikos veiksniams vertinti naudojama dvidešimt penkių balų rizikos vertinimo sistema, pagal kurią, nustačius rizikos veiksnių tikimybę ir poveikį, apskaičiuojamas rizikos laipsnis:

22.1. rizikos laipsnis nuo 1 iki 6 – maža rizika;

22.2. rizikos laipsnis nuo 8 iki 12 – vidutinė rizika;

22.3. rizikos laipsnis nuo 15 iki 25 – didelė rizika.

23. Kuo didesnė rizikos veiksnio tikimybė ir jo poveikis, tuo rizikos laipsnis aukštesnis. Rizikos veiksniams, kuriems nustatytas aukštas rizikos laipsnis, būtina skirti didžiausią dėmesį parenkant ir įgyvendinant tinkamas rizikos mažinimo priemones.

24. Informacinės sistemos rizikos įvertinimo rezultatai ir priemonės rizikos veiksniams išvengti išdėstomi Rizikos įvertinimo ataskaitoje, kuri pateikiama Informacinės sistemos pagrindinio tvarkytojo vadovui. Rizikos veiksniai rizikos įvertinimo ataskaitoje turi būti išdėstyti pagal prioritetus ir priimtiną rizikos lygį.

25. Atsižvelgdamas į rizikos vertinimo ataskaitą, Informacinės sistemos valdytojas prireikus tvirtina rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių, organizacinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

26. Siekiant įvertinti Informacinės sistemos saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, kartą per metus, jei teisės aktuose nenustatyta kitaip, organizuojamas informacinių technologijų saugos atitikties vertinimas.

27. Informacinių technologijų saugos atitikties vertinimo metodikoje nustatyta tvarka atlikus informacinių technologijų saugos atitikties vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita, kuri pateikiama Informacinės sistemos pagrindinio tvarkytojo vadovui, ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus jo vykdytojus paskiria ir įgyvendinimo terminus nustato Informacinės sistemos valdytojo vadovas.

28. Informacinės sistemos atitikties Organizacinių ir techninių kibernetinio saugumo reikalavimų apraše nustatytiems organizaciniams ir techniniams kibernetinio saugumo reikalavimams vertinimas turi būti organizuojamas ne rečiau kaip kartą per metus.

29. Informacinės sistemos rizikos įvertinimo ataskaitos, Informacinės sistemos rizikos įvertinimo ir rizikos valdymo priemonių plano, Informacinės sistemos informacinių technologijų saugos atitikties vertinimo ataskaitos, taip pat pastebėtų trūkumų šalinimo plano kopijas Informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų, patvirtintų Lietuvos Respublikos krašto apsaugos ministro 2018 m. gruodžio 11 d. įsakymu Nr. V-1183 „Dėl Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemos nuostatų patvirtinimo“, nustatyta tvarka (jeigu Informacinė sistema priskiriama valstybės informaciniams ištekliams).

30. Elektroninės informacijos saugos (kibernetinio saugumo) priemonės (techninės, programinės, organizacinės ir kitos informacinių sistemų elektroninės informacijos saugos (kibernetinio saugumo) priemonės) parenkamos vadovaujantis šiais principais:

30.1. liekamoji rizika turi būti sumažinta iki priimtino lygio;

30.2. priemonės diegimo kaina turi būti adekvati tvarkomos elektroninės informacijos vertei;

30.3. kur galima, turi būti įdiegiamos prevencinės, detekcinės ir korekcinės informacijos saugos (kibernetinio saugumo) priemonės.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

31. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai nustatomi pagal Saugos nuostatų 17 ir 18 punktuose nustatytas Informacinės sistemos svarbos kategorijas ir vadovaujantis Saugos nuostatų 16 punkte nurodytais teisės aktais ir standartais.

32. Kibernetinio saugumo priemonės, nurodytos Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo priede, turi būti diegiamos atsižvelgiant į naujausius technikos laimėjimus, vadovaujantis gamintojo pateikiama bent viena gerosios saugumo praktikos rekomendacija.

33. Organizacinių ir techninių elektroninės informacijos saugos (kibernetinio saugumo) priemonių užtikrinimas turi būti grindžiamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos

Informacinės sistemos elektroninės informacijos saugai (kibernetiniam saugumui), rizikos vertinimu, atsižvelgiant į naujausius technikos laimėjimus.

34. Programinės įrangos, skirtos Informacinei sistemai nuo kenksmingos programinės įrangos (virusų, programinės įrangos, skirtos šnipinėjimui, nepageidaujamo elektroninio pašto ir panašiai) apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai:

34.1. Informacinės sistemos tarnybinių stočių ir kompiuterinėse darbo vietose turi būti įdiegtos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios turi būti reguliariai ir operatyviai atnaujinamos automatiniu būdu;

34.2. turi būti naudojamos priemonės, turinčios apsaugos mechanizmus, blokuojančius kenkimo programų bandymus panaikinti apsaugas nuo kenkimo programų.

35. Detalios programinės įrangos, skirtos Informacinei sistemai nuo kenksmingos programinės įrangos apsaugoti, naudojimo nuostatos ir jos atnaujinimo reikalavimai (ilgiausias leistinas neatnaujinimo laikas ir kt.), nustatomi Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

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

36.1. turi būti naudojama tik legali Informacinės sistemos funkcijoms vykdyti būtina programinė įranga;

36.2. programinė įranga turi būti nuolatos atnaujinama laikantis gamintojo reikalavimų;

36.3. turi būti įdiegta prieigos prie Informacinės sistemos elektroninės informacijos per registravimą, teisių suteikimą ir slaptažodžius sistema;

36.4. turi būti įgyvendinta prievolė keisti slaptažodžius ne rečiau kaip kas 3 mėnesius;

36.5. turi būti įdiegta galimybė fiksuoti ir kaupti informaciją apie asmenų, kurie naudojosi prieiga prie Informacinės sistemos elektroninės informacijos, atliktus veiksmus.

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

37.1. Informacinės sistemos elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienes, ugniasienių įvykių žurnalai turi būti reguliariai analizuojami;

37.2. Informacinės sistemos programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: DDoS atakų, nestandartinių protokolų naudojimo, internetinės žvalgybos (informacijos rinkimo per laisvai platinamas programas), slaptažodžių atakų (Brute Force Attack, Fishing);

37.3. Informacinės sistemos tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo.

38. Detalios kompiuterių tinklo filtravimo įrangos naudojimo nuostatos nustatomos Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

39. Leistinos kompiuterių naudojimo ribos:

39.1. stacionarūs ir nešiojamieji Informacinės sistemos naudotojų kompiuteriai ir kiti mobilieji įrenginiai turi būti naudojami tik tiesioginėms pareigoms atlikti. Iš kompiuterių, kurie perduodami remontuoti ar techninei priežiūrai atlikti, turi būti pašalinti visi Informacinės sistemos duomenys ir informacija;

39.2. nešiojamuosiuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose turi būti taikomos papildomos saugos priemonės (elektroninės informacijos šifravimas, prisijungimo ribojimas ir pan.);

39.3. Informacinės sistemos naudotojai privalo naudotis visomis saugumo priemonėmis, kad apsaugotų kompiuterį ir duomenų laikmenas nuo vagystės arba pažeidimo.

40. Metodai, kuriais užtikrinamas saugus Informacinės sistemos elektroninės informacijos teikimas ir (ar) gavimas:

40.1. elektroninė informacija iš susijusių registrų, informacinių sistemų gaunama ir teikiama susijusiems registrams, informacinėms sistemoms tik pagal duomenų teikimo ir gavimo sutartyse nustatytas perduodamų duomenų specifikacijas, perdavimo sąlygas ir tvarką;

40.2. prieigos prie Informacinės sistemos elektroninės informacijos, teises gali suteikti tik Informacinės sistemos administratorius. Informacinės sistemos naudotojams suteikiamos tik jų funkcijoms vykdyti būtinos teisės;

40.3. prieiga prie Informacinės sistemos elektroninės informacijos leidžiama tik per registravimosi slaptažodžių sistemą. Prieigos prie Informacinės sistemos elektroninės informacijos valdymas apibrėžtas Informacinės sistemos naudotojų administravimo taisyklėse;

40.4. pasibaigus Informacinės sistemos naudotojo darbo sutarčiai, teisė naudotis Informacinės sistemos elektronine informacija turi būti panaikinta. Informacinės sistemos naudotojui prieiga prie Informacinės sistemos turi būti ribojama ar sustabdoma, kai vyksta Informacinės sistemos naudotojo veiklos tyrimas, naudotojas turi ilgalaikes atostogas arba keičiasi jo atliekamos ir (ar) pareigybės aprašyme nurodytos funkcijos.

41. Informacinės sistemos atsarginės kopijos daromos automatiniu būdu, vieną kartą per parą. Kopijos saugomos 2 atskiruose geografiškai atskirtuose duomenų centruose naudojant 256 bitų AES šifravimą ir saugomos 7 dienas. Duomenų bazės atsarginės kopijos daromos bent kartą per 5 minutes ir taip pat saugomos atskiruose duomenų centruose.

42. Prireikus atkurti kopijas teisę tam turi tik Informacinės sistemos administratorius ar jį pavaduojantis asmuo. Periodiškai, bet ne rečiau kaip kartą per pusmetį turi būti atliekami elektroninės informacijos atkūrimo iš atsarginių kopijų bandymai.

43. Kopijų darymo ir saugojimo tvarka nustatoma Informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklėse.

44. Organizaciniai ir techniniai elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai detalizuojami Informacinės sistemos saugos (kibernetinio saugumo) politiką įgyvendinančiuose dokumentuose.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

45. Saugos įgaliotinis privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, tobulinti elektroninės informacijos saugos (kibernetinio saugumo) srities kvalifikaciją, savo darbe vadovautis Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Organizacinių ir techninių kibernetinio saugumo reikalavimų aprašo ir kitų Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą (kibernetinį saugumą). Informacinės sistemos pagrindinis tvarkytojas turi sudaryti sąlygas saugos įgaliotiniui kelti kvalifikaciją.

46. Saugos įgaliotiniu 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 prijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

47. Informacinės sistemos administratoriai pagal kompetenciją privalo išmanyti elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo principus, mokėti užtikrinti Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą), administruoti ir prižiūrėti Informacinės sistemos komponentus (stebėti Informacinės sistemos komponentų veikimą, atlikti jų profilaktinę priežiūrą, trikčių diagnostiką ir šalinimą, sugebėti užtikrinti Informacinės sistemos komponentų nepertraukiamą funkcionavimą ir pan.). Informacinės sistemos administratoriai turi būti susipažinę su saugos dokumentais.

48. Informacinės sistemos naudotojai privalo turėti pagrindinius darbo kompiuteriu, taikomosiomis programomis įgūdžius, mokėti tvarkyti elektroninę informaciją, būti susipažinę su Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymu, kitais teisės aktais, reglamentuojančiais asmens duomenų tvarkymą, informacinių sistemų elektroninės informacijos tvarkymą. Asmenys, tvarkantys duomenis ir informaciją, privalo laikyti jų paslaptį ir būti pasirašę pasižadėjimą saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su elektroninės informacijos tvarkymu susijusią veiklą.

49. Informacinės sistemos naudotojų, administratorių, saugos įgaliotinio kvalifikacija turi atitikti reikalavimus, nustatytus jų pareiginiuose nuostatuose ar pareigybės aprašyme.

50. Informacinės sistemos naudotojų ir Informacinės sistemos administratorių mokymo planavimo, organizavimo ir vykdymo tvarka, mokymo periodiškumo reikalavimai:

50.1. Informacinės sistemos naudotojams turi būti įvairiais būdais primenama apie elektroninės informacijos saugos (kibernetinio saugumo) problemas (pvz., priminimai elektroniniu paštu, teminių renginių organizavimas, atmintinės naujiems informacinių sistemų naudotojams, Informacinių sistemų administratoriams ir pan.);

50.2. mokymai elektroninės informacijos saugos (kibernetinio saugumo) klausimais turi būti planuojami ir mokymo būdai parenkami atsižvelgiant į elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo prioritetines kryptis ir tikslus, įdiegtas ar planuojamas įdiegti technologijas (techninę ar programinę įrangą), saugos įgaliotinio, Informacinės sistemos naudotojų ar Informacinių sistemų administratorių poreikius;

50.3. mokymai gali būti vykdomi tiesioginiu (pvz., paskaitos, seminarai, konferencijos ir kt. teminiai renginiai) ar nuotoliniu būdu (pvz., vaizdo konferencijos, mokomosios medžiagos pateikimas elektroninėje erdvėje ir pan.);

50.4. mokymai Informacinės sistemos naudotojams turi būti organizuojami periodiškai, bet ne rečiau kaip kartą per metus. Už mokymų organizavimą atsakingas Informacinės sistemos saugos įgaliotinis. Mokymai Informacinės sistemos saugos įgaliotiniui ir Informacinės sistemos administratoriams turi būti organizuojami pagal poreikį.

V SKYRIUS
INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

51. Informacinės sistemos naudotojus su Saugos nuostatais ir saugos dokumentais ir atsakomybe už jų reikalavimų nesilaikymą supažindina Informacinės sistemos saugos įgaliotinis arba naudotojai supažindinami informacinės sistemos priemonėmis. Informacinės sistemos naudotojai, pažeidę Saugos nuostatų reikalavimus, atsako teisės aktų nustatyta tvarka.

52. Pakartotinai su Saugos nuostatais ir saugos dokumentais Informacinės sistemos naudotojai supažindinami jiems pasikeitus.

53. Saugos nuostatai bei kiti dokumentai, reglamentuojantys saugų elektroninės informacijos tvarkymą, skelbiami Informacinės sistemos pagrindinio tvarkytojo interneto svetainėje ar kitais būdais.

54. Informacinės sistemos naudotojų supažindinimo su Saugos nuostatais ir saugos dokumentais tvarka nustatyta Informacinės sistemos naudotojų administravimo taisyklėse.

55. Tvarkyti Informacinės sistemos elektroninę informaciją gali tik Informacinės sistemos naudotojai, kurie yra susipažinę su saugos dokumentais ir sutikę laikytis jų reikalavimų. Informacinės sistemos naudotojai atsako už Informacinės sistemos ir joje tvarkomos elektroninės informacijos saugą (kibernetinį saugumą) pagal savo kompetenciją.

56. Informacinės sistemos naudotojai, Informacinės sistemos administratoriai ir saugos įgaliotinis, pažeidę saugos dokumentų ir kitų saugų elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako Lietuvos Respublikos įstatymų nustatyta tvarka.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

57. Informacinės sistemos valdytojas saugos dokumentus gali keisti savo arba saugos įgaliotinio iniciatyva. Saugos dokumentai turi būti derinami su Nacionaliniu kibernetinio saugumo centru. Keičiami saugos dokumentai gali būti nederinami su Nacionaliniu kibernetinio saugumo centru tais atvejais, kai atliekami tik redakciniai ar nežymūs nustatyto teisinio reguliavimo esmės ar elektroninės informacijos saugos politikos ir kibernetinio saugumo politikos nekeičiantys pakeitimai arba taisoma teisės technika. Tokiais atvejais Nacionaliniam kibernetinio saugumo centrui turi būti pateiktos šių dokumentų kopijos.

58. Saugos nuostatai ir saugos dokumentai iš esmės turi būti persvarstomi (peržiūrimi) ne rečiau kaip kartą per kalendorinius metus. Saugos dokumentai taip pat turi būti persvarstomi (peržiūrimi) atlikus rizikos veiksnių analizę ar informacinių technologijų saugos atitikties vertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams.

Pakeitimai:

1.
Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras, Įsakymas
Nr. 05-45, 2021-05-07, paskelbta TAR 2021-05-10, i. k. 2021-10315
Dėl Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro direktoriaus 2021 balandžio 8 d. įsakymo Nr. 05-36 „Dėl Ekstremalių situacijų valdymo informacinės sistemos nuostatų ir Ekstremalių situacijų valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo

2.
Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras, Įsakymas
Nr. 05-50, 2021-05-29, paskelbta TAR 2021-05-31, i. k. 2021-12139
Dėl Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro direktoriaus 2021 m. balandžio 8 d. įsakymo Nr. 05-36 „Dėl Ekstremalių situacijų valdymo informacinės sistemos nuostatų ir Ekstremalių situacijų valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo

3.
Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras, Įsakymas
Nr. 05-61, 2021-06-21, paskelbta TAR 2021-06-22, i. k. 2021-14085
Dėl Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro direktoriaus 2021 m. balandžio 8 d. įsakymo Nr. 05-36 „Dėl Ekstremalių situacijų valdymo informacinės sistemos nuostatų ir Ekstremalių situacijų valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo

4.
Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras, Įsakymas
Nr. 05-113, 2021-11-30, paskelbta TAR 2021-12-01, i. k. 2021-24809
Dėl Sveikatos apsaugos ministerijos ekstremalių sveikatai situacijų centro direktoriaus 2021 m. balandžio 8 d. įsakymo Nr. 05-36 „Dėl Ekstremalių situacijų valdymo informacinės sistemos nuostatų ir Ekstremalių situacijų valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo

5.
Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centras, Įsakymas
Nr. V-87, 2023-07-28, paskelbta TAR 2023-07-28, i. k. 2023-15435
Dėl Sveikatos apsaugos ministerijos Ekstremalių sveikatai situacijų centro direktoriaus 2021 m. balandžio 8 d. įsakymo Nr. 05-36 „Dėl Ekstremalių situacijų valdymo informacinės sistemos nuostatų ir Ekstremalių situacijų valdymo informacinės sistemos duomenų saugos nuostatų patvirtinimo“ pakeitimo