Suvestinė redakcija nuo 2023-12-22

Įsakymas paskelbtas: TAR 2021-04-06, i. k. 2021-07096

UŽIMTUMO TARNYBOS
PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS
IR DARBO MINISTERIJOS
DIREKTORIUS

ĮSAKYMAS
DĖL UŽIMTUMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATŲ IR ELEKTRONINĖS INFORMACIJOS SAUGOS POLITIKĄ ĮGYVENDINANČIŲ DOKUMENTŲ PATVIRTINIMO

2021 m. kovo 19 d. Nr. V-113
Vilnius

Vadovaudamasi Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, 7, 8, 12 ir 13 punktais:

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

1.1. Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų duomenų saugos nuostatus;

1.2. Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos saugaus elektroninės informacijos tvarkymo taisykles;

1.3. Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų veiklos tęstinumo valdymo planą;

1.4. Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų naudotojų administravimo taisykles.

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

2.1. Lietuvos darbo biržos prie Socialinės apsaugos ir darbo ministerijos direktoriaus 2010 m. rugsėjo 22 d. įsakymą Nr. V-509 „Dėl Lietuvos darbo biržos informacinės sistemos duomenų saugos nuostatų patvirtinimo“ su visais pakeitimais ir papildymais;

2.2. Lietuvos darbo biržos prie Socialinės apsaugos ir darbo ministerijos direktoriaus 2014 m. rugpjūčio 22 d. įsakymą Nr. V-512 „Dėl Lietuvos darbo biržos informacinės sistemos saugos politiką įgyvendinančių dokumentų patvirtinimo“ su visais pakeitimais ir papildymais;

2.3. Lietuvos darbo biržos prie Socialinės apsaugos ir darbo ministerijos direktoriaus 2017 m. sausio 18 d. įsakymą Nr. V-43 „Dėl Lietuvos darbo biržos personalo valdymo informacinės sistemos saugos politiką gyvendinančių dokumentų patvirtinimo“ su visais pakeitimais ir papildymais.

3. P a v e d u Teisės skyriui organizuoti šio įsakymo paskelbimą Teisės aktų registre ir Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos interneto svetainėje.

Direktorė Inga Balnanosienė

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2021 m. kovo 2 d. raštu Nr. (4.1 E) 6K-153

PATVIRTINTA
Užimtumo tarnybos prie Lietuvos Respublikos
socialinės apsaugos ir darbo ministerijos direktoriaus
2021 m. kovo 19 d. įsakymu Nr. V-113
(Užimtumo tarnybos prie Lietuvos Respublikos
socialinės apsaugos ir darbo ministerijos direktoriaus
2022 m. rugsėjo 27 d.
įsakymo Nr. V-298 redakcija)

UŽIMTUMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų duomenų saugos nuostatai (toliau – Saugos nuostatai) reglamentuoja Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos (toliau – Užimtumo tarnyba, Įstaiga) informacijos saugos ir kibernetinio saugumo politiką (toliau – Saugos politika), apibrėžia pagrindinius elektroninės informacijos saugos užtikrinimo ir valdymo principus, nustato organizacinius ir techninius informacijos saugos ir kibernetinio saugumo reikalavimus (toliau kartu – saugos reikalavimai), taikomus Užimtumo tarnybos valdomoms informacinėms sistemoms (toliau – Įstaigos IS), nurodytoms Saugos nuostatų 1 priede.

2. Saugos politika Įstaigoje įgyvendinama vadovaujantis šiais Saugos nuostatais, Saugaus elektroninės informacijos tvarkymo taisyklėmis, Naudotojų administravimo taisyklėmis, Veiklos tęstinumo valdymo planu (toliau kartu – Saugos dokumentai) bei kitomis Įstaigos taisyklėmis, aprašais, procedūromis bei dokumentais, reglamentuojančiais informacijos saugą ir kibernetinį saugumą.

3. Saugos nuostatai parengti vadovaujantis šiais teisės aktais:

3.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

3.2. Lietuvos Respublikos kibernetinio saugumo įstatymu;

3.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo” (toliau – Kibernetinio saugumo reikalavimų aprašas);

3.4. 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 – Bendrųjų saugos reikalavimų aprašas);

3.5. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu 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 – Techninių saugos reikalavimų aprašas);

3.6. Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2003 m. balandžio 18 d. nutarimu Nr. 480 „Dėl Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms aprašo patvirtinimo“.

4. Įstaigos valdomose informacinėse sistemose asmens duomenys tvarkomi ir tvarkomų asmens duomenų saugumas užtikrinamas vadovaujantis 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), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo ir kitų teisės aktų, reglamentuojančių asmens duomenų apsaugą, reikalavimais.

5. Saugos nuostatuose vartojamos sąvokos:

5.1. **Saugos įgaliotinis** – Užimtumo tarnybos direktoriaus įsakymu paskirtas Įstaigos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį (toliau – darbuotojas) atsakingas už Įstaigos informacijos saugos politikos įgyvendinimą, koordinavimą ir priežiūrą bei įgyvendina už kibernetinio saugumo organizavimą ir užtikrinimą Įstaigoje atsakingo asmens funkcijas, t. y. atsako už kibernetinio saugumo organizavimą ir užtikrinimą Užimtumo tarnyboje bei dalyvauja kibernetinių incidentų valdyme;

5.2. **Įstaigos IS** – Užimtumo tarnybos nustatytoms funkcijoms vykdyti ir atlikti reikalinga, informaciją apdorojanti teisinių, organizacinių, techninių ir programinių priemonių visuma, skirta Įstaigos uždaviniams ir funkcijoms įgyvendinti naudojant informacines ir ryšių technologijas;

5.3. **Įstaigos IS administratorius** – Užimtumo tarnybos direktoriaus įsakymu paskirtas darbuotojas, prižiūrintis Įstaigos IS ir (ar) jų infrastruktūrą, užtikrinantis jų veikimą ir atliekantis funkcijas, susijusias su Įstaigos IS naudotojų teisių valdymu, Įstaigos IS komponentais

(kompiuteriais, operacinėmis sistemomis, duomenų bazių valdymo sistemomis, taikomųjų programų sistemomis, ugniasienėmis, įsilaužimų aptikimo sistemomis, elektroninės informacijos perdavimu tinklais, bylų serveriais ir kitais), šių informacinių sistemų komponentų sąranka, pažeidžiamų vietų nustatymu, saugumo reikalavimų atitikties nustatymu ir stebėsena, reagavimu į elektroninės informacijos saugos ir kibernetinio saugumo incidentus (toliau – kibernetiniai incidentai); arba kitas trečiasis asmuo (asmenų grupė), kuriam (kuriai) teisės aktų nustatyta tvarka ir pagrindais yra perduotos Įstaigos IS ir (arba) jos infrastruktūros priežiūros ir (arba) administravimo funkcijos;

5.4. **Įstaigos IS naudotojas** – Užimtumo tarnybos darbuotojas, Įstaigos IS veiklą reglamentuojančių teisės aktų nustatyta tvarka atliekant priskirtas tarnybines ar darbo funkcijas pagal kompetenciją naudojantis ir tvarkantis elektroninę informaciją;

5.5. **Įstaigos IS vartotojas** – fizinis asmuo, veikiantis savo arba atstovaujamo juridinio asmens interesais, kuriam Užimtumo tarnybos teikiamos viešosios ir (arba) administracinės paslaugos teikiamos naudojantis Įstaigos IS.

6. Kitos Saugos nuostatuose vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Saugos nuostatų 3 punkte nurodytuose teisės aktuose ir Lietuvos Respublikos standartuose LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ bei LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“.

7. Saugos nuostatų 1 priede nurodytų Įstaigos IS valdytojas ir tvarkytojas yra Užimtumo tarnyba, buveinės adresas: Geležinio Vilko g. 3A, LT-03131 Vilnius.

8. Saugos nuostatai privalomi ir taikomi Įstaigos IS valdytojui, tvarkytojui, saugos įgaliotiniui, Įstaigos IS administratoriams, Įstaigos IS naudotojams, Įstaigos IS vartotojams bei tretiesiems asmenims, kuriems teisės aktų nustatyta tvarka suteiktos prieigos teisės prie Užimtumo tarnybos informacinių sistemų ir informacijos arba, kurie teikia Įstaigos IS infrastruktūros, kompiuterinės įrangos saugos ir priežiūros paslaugas.

9. Užimtumo tarnyba, kaip Įstaigos IS valdytoja, yra atsakinga už Saugos politikos Įstaigoje formavimą ir įgyvendinimą bei atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi. Vykdydama valdytojui priskirtas funkcijas Užimtumo tarnyba:

9.1. rengia ir tvirtina Įstaigos IS Saugos dokumentus ir kitus informacijos saugos ir kibernetinio saugumo politiką įgyvendinančius teisės aktus;

9.2. kontroliuoja kaip laikomasi Saugos dokumentų ir kitų teisės aktų, reglamentuojančių

Įstaigos IS informacijos saugą ir kibernetinį saugumą;

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

9.4. skiria saugos įgaliotinį ar įgaliotinius ir Įstaigos IS administratorių ar administratorius arba sudaro sutartį su išoriniu paslaugų teikėju dėl Įstaigos IS administratoriaus funkcijų vykdymo perdavimo;

9.5. atsako už Įstaigos IS duomenų tvarkymo ir duomenų teikimo/gavimo teisėtumą ir saugą;

9.6. priima sprendimą dėl Įstaigos IS informacinių technologijų saugos reikalavimų atitikties vertinimo atlikimo ir informacinių sistemų rizikos vertinimo atlikimo;

9.7. vykdo kitas IS valdytojui priskirtas funkcijas.

10. Užimtumo tarnyba kaip Įstaigos IS tvarkytojas atsako už reikiamų administracinių, techninių ir organizacinių saugos priemonių įgyvendinimą, užtikrinimą ir laikymąsi Saugos dokumentuose nustatyta tvarka.

11. Saugos įgaliotinis:

11.1. teikia Užimtumo tarnybos direktoriui pasiūlymus dėl:

11.1.1. Įstaigos IS administratoriaus ar administratorių paskyrimo ar administravimo funkcijų perdavimo tretiesiems asmenims ir Įstaigos IS administratoriams taikomų reikalavimų nustatymo;

11.1.2. informacinių technologijų saugos atitikties ir rizikos vertinimo atlikimo;

11.1.3. Saugos dokumentų priėmimo, keitimo ir panaikinimo;

11.2. koordinuoja kibernetinių incidentų tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų, informacijos saugos ir kibernetinio saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos (kibernetinio saugumo) incidentais;

11.3. teikia Įstaigos IS administratoriui (administratoriams) ir Įstaigos IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Saugos nuostatų ir kitų Saugos dokumentų ir juose nustatytų saugos reikalavimų įgyvendinimu;

11.4. organizuoja naudotojų supažindinimą su Saugos dokumentais bei užtikrina supažindinimo įrodomumą;

11.5. koordinuoja Saugos dokumentų reikalavimų vykdymą;

11.6. organizuoja rizikos ir informacinių technologijų saugos atitikties vertinimą, o Įstaigos direktoriaus pavedimu – ir atlieka juos;

11.7. organizuoja Įstaigos IS naudotojams mokymus ir (arba) kursus elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo klausimais, kelia naudotojų žinių lygį informuodamas apie informacijos saugos ir kibernetinio saugumo problematiką, naujas grėsmes bei apsaugos nuo grėsmių būdus siųsdamas atmintines ar priminimus elektroniniu paštu ar patalpindamas aktualią informaciją Įstaigos intranete;

11.8. teikia Įstaigos IS tvarkytojams metodinę ir informacinę medžiagą informacijos saugos ir kibernetinio saugumo klausimais, apibendrina duomenų registravimo, keitimo, išregistravimo ir kitų su duomenimis atliekamų veiksmų praktiką ir teikia bendrą praktiką formuojančias rekomendacijas;

11.9. atlieka kitas Bendrųjų saugos reikalavimų apraše, Kibernetinio saugumo reikalavimų apraše, šiuose Saugos nuostatuose, Saugos dokumentuose bei kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą ir kibernetinį saugumą, saugos įgaliotiniui ir už kibernetinio saugumo organizavimą atsakingam asmeniui priskirtas funkcijas.

12. Saugos įgaliotinis negali atlikti Įstaigos IS administratoriaus funkcijų.

13. Įstaigos IS administratorių (administratorius) Saugos įgaliotinio teikimu skiria Užimtumo tarnybos direktorius. Valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatyta tvarka administratoriaus funkcijų vykdymas gali būti perduodamas išoriniam paslaugos teikėjui.

14. Įstaigos IS administratoriaus teisės gali būti suteikiamos tik informacinių sistemų priežiūros funkcijoms atlikti, Įstaigos IS administratoriaus paskyra negali būti naudojama atliekant Įstaigos IS naudotojo funkcijas.

15. Įstaigos IS administratorius (administratoriai) atlieka šias funkcijas:

15.1. atsako už Įstaigos IS funkcionavimą užtikrinančios techninės ir programinės įrangos, infrastruktūros bei informacinių technologijų paslaugų administravimą;

15.2. registruoja Įstaigos IS naudotojus ir suteikia prieigos teises naudotis Įstaigos IS infrastruktūra paskirtoms funkcijoms atlikti;

15.3. rengia ir teikia pasiūlymus Įstaigos IS valdytojui dėl Įstaigos IS kūrimo, palaikymo, priežiūros, techninės ir programinės įrangos modernizavimo ir duomenų saugos užtikrinimo;

15.4. atlieka Įstaigos IS sudarančių komponentų (kompiuterių, operacinių sistemų, duomenų bazių valdymo sistemų, taikomųjų programų sistemų, ugniasienių, įsilaužimų aptikimo sistemų, duomenų perdavimo tinklų ir kitų komunikavimo priemonių) administravimą, užtikrina jų tinkamą

funkcionavimą, pažeidžiamų vietų nustatymą ir saugos priemonių parinkimą bei atsako už jų atitiktį Užimtumo tarnybos Saugos dokumentų reikalavimams;

15.5. administruoja Įstaigos IS duomenų bazes, kontroliuoja duomenų įvedimo funkcionalumo teisingumą, nustato galimas sutrikimų priežastis;

15.6. atlieka Įstaigos IS pažeidžiamų vietų nustatymą, Saugos reikalavimų atitikties nustatymą ir stebėseną, reaguoja į kibernetinius incidentus, nedelsiant informuoja saugos įgaliotinį apie įvykusius kibernetinius incidentus bei teikia pasiūlymus dėl priemonių kibernetinių incidentų šalinimui taikymo;

15.7. atlieka kitas Saugos dokumentuose priskirtas funkcijas, vykdo saugos įgaliotinio nurodymus ir pavedimus, susijusius su Įstaigos IS saugos užtikrinimu, nuolat teikia saugos įgaliotiniui informaciją apie Įstaigos IS saugos būklę.

II SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

16. Įstaigos IS tvarkomos informacijos svarba bei priskyrimo konkrečios svarbos lygiui kriterijai, Įstaigos IS kategorijos, ilgiausias leistinas konkrečių informacinių sistemų sutrikimo laikotarpis ir kita su Įstaigos IS susijusi informacija pateikiama Saugos nuostatų 1 priede.

17. Įstaigos IS tvarkomos elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo tikslai:

17.1. sudaryti sąlygas saugiai automatizuotu būdu tvarkyti Įstaigos IS elektroninę informaciją;

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

17.3. vykdyti kibernetinių incidentų prevenciją, reaguoti į kibernetinius incidentus ir juos operatyviai suvaldyti, atkuriant įprastą Įstaigos IS veiklą ir Įstaigos funkcijų vykdymą.

18. Elektroninės informacijos sauga ir kibernetinis saugumas turi būti įgyvendinamas taikant elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo priemones (toliau – Saugos priemonės), nurodytas šiuose Saugos nuostatuose bei kituose Saugos dokumentuose. Saugos priemonės turi būti parenkamos ir diegiamos atsižvelgiant į Įstaigos IS kylančią riziką, nustatytą rizikos vertinimo metu bei atsižvelgiant į naujausius technikos laimėjimus.

19. Pagrindiniai Saugos priemonių parinkimo principai yra šie:

19.1. Įstaigos IS likutinė rizika turi būti sumažinta iki priimtino lygio;

19.2. diegimo kainos adekvatumas saugomos informacijos vertei;

19.3. turi būti įdiegtos prevencinės, detekcinės ir korekcinės saugos priemonės.

20. Siekiant užtikrinti Saugos reikalavimų įgyvendinimo organizavimą ir kontrolę ne rečiau kaip kartą per metus turi būti organizuojamas informacinių technologijų saugos atitikties saugumo reikalavimams vertinimas (toliau – atitikties vertinimas) ir Įstaigos IS rizikos vertinimas (toliau – rizikos vertinimas). Atsižvelgiant į Įstaigoje įvykius pokyčius, grėsmes, įvykusius kibernetinius incidentus bei kitą informaciją, gali būti organizuojamas neeilinis rizikos vertinimas.

21. Atliekant atitikties vertinimą turi būti atliekami šie veiksmai:

21.1. sudaromas Įstaigos IS privalomų taikyti saugos reikalavimų sąrašas bei įvertinamas saugos reikalavimų įgyvendinimo lygis;

21.2. inventorizuojama Įstaigos IS techninė ir programinė įranga;

21.3. patikrinama atsitiktinai parinktų Įstaigos IS naudotojų kompiuterizuotų darbo vietų, visose informacinės sistemos tarnybinėse stotyse įdiegtos programos ir jų sąranka;

21.4. patikrinama Įstaigos IS naudotojams suteiktų teisių ir vykdomų funkcijų atitiktis Saugos dokumentuose nustatytiems reikalavimams;

21.5. įvertinamas pasirengimas užtikrinti Įstaigos IS veiklos tęstinumą, įvykus kibernetiniam incidentui;

21.6. peržiūrimi Saugos dokumentai, įvertinama jų atitiktis teisės aktų reikalavimams bei, esant poreikiui, parengiami Saugos dokumentų pakeitimai.

22. Saugos įgaliotinis atsakingas už rizikos vertinimą, rizikos vertinimo proceso priežiūrą bei nuolatinį tobulinimą. Užimtumo tarnybos direktoriaus sprendimu rizikos vertinimo proceso priežiūros bei nuolatinio tobulinimo paslaugos gali būti pavestos trečiajam asmeniui.

23. Rizikos vertinimas, atliekamas atsižvelgiant į Nacionalinio kibernetinio saugumo centro prie Lietuvos Respublikos krašto apsaugos ministerijos interneto svetainėje skelbiamą metodinę priemonę „Rizikos analizės vadovas“, taip pat į Lietuvos ir tarptautinius standartus ar metodikas, reglamentuojančias rizikos valdymą.

24. Atliekant rizikos vertinimą turi būti organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos Įstaigos IS elektroninės informacijos saugai ir kibernetiniam saugumui vertinimas. Rizikos vertinimo metu turi būti:

24.1. sudaromas vertintinų informacinių išteklių sąrašas;

24.2. nustatomi esami informacinių išteklių pažeidžiamumai;

24.3. atliekamas grėsmių ir jų tikimybės įvertinimas;

24.4. atliekamas rizikos veiksnių įtakos vertinimas;

24.5. nustatomas rizikos lygis, priimtina rizika;

24.6. parenkami nepriimtinos rizikos valdymo būdai/priemonės;

24.7. parengiama rizikos vertinimo ataskaita ir nepriimtinos rizikos valdymo priemonių planas.

25. Rizikos vertinimo rezultatai išdėstomi rizikos vertinimo ataskaitoje, kurioje įvertinami rizikos veiksniai, galintys turėti įtakos elektroninės informacijos saugai, jų galima žala, pasireiškimo tikimybė ir pobūdis, galimi rizikos valdymo būdai bei rizikos priimtinumo kriterijai. Kartu su rizikos vertinimo ataskaita turi būti parengiamas nepriimtinos rizikos valdymo priemonių planas.

26. Rizikos vertinimo metu nustatant vertinimo apimtį turi būti parengiamas pažeidžiamumų nustatymo planas, kuris turi apimti pažeidžiamumų nustatymo būdą – ar bus atliekamas savo jėgomis, ar pasitelkiant išorinius paslaugų teikėjus.

27. Atlikus technologinio pažeidžiamumo vertinimą turi būti parengta detali ataskaita, kurioje turi būti pateikiamas trumpas atlikto technologinio pažeidžiamumų vertinimo aprašymas ir jo atlikimo tikslas, nurodyta, kas buvo testuota, testavimo rezultatai ir nustatyti pažeidžiamumai bei rekomendacijos nustatytų pažeidžiamumų pašalinimui.

28. Atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijos, rizikos vertinimo ataskaitos, rizikos vertinimo ir rizikos valdymo priemonių plano kopijos ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi būti 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.

III SKYRIUS
ORGANIZACINIAI IR TECHNINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI

29. Įstaigos IS informacijos saugai (kibernetiniam saugumui) užtikrinti naudojamos organizacinės, techninės, programinės ir fizinės informacijos apsaugos priemonės.

30. Programinės įrangos, skirtos Įstaigos IS apsaugoti nuo kenksmingos programinės įrangos (virusų, šnipinėjimo programinės įrangos, nepageidaujamo elektroninio pašto ir pan.), naudojimo sąlygos ir jos atnaujinimo reikalavimai:

30.1. tarnybinėse stotyse ir naudotojų kompiuterinėse darbo vietose turi būti naudojamos centralizuotai valdomos ir atnaujinamos kenksmingos programinės įrangos aptikimo, stebėjimo realiu laiku priemonės;

30.2. Įstaigos IS komponentai be kenksmingos programinės įrangos aptikimo priemonių

gali būti eksploatuojami, jeigu rizikos vertinimo metu patvirtinama, kad šių komponentų rizika yra priimtina;

30.3. kenksmingos programinės įrangos aptikimo priemonės turi atsinaujinti automatiškai ne rečiau kaip kartą per dieną. Įstaigos IS administratoriai turi būti automatiškai informuojami elektroniniu paštu apie tai, jog yra pradelstas kenksmingos programinės įrangos aptikimo priemonių atsinaujinimo laikas, kenksmingos programinės įrangos aptikimo priemonės netinkamai funkcionuoja arba yra išjungtos.

31. Programinės įrangos, įdiegtos kompiuteriuose ir tarnybinėse stotyse, naudojimo sąlygos:

31.1. turi būti naudojama tik legali Įstaigos IS funkcijoms vykdyti būtina programinė įranga;

31.2. saugos įgaliotinis periodiškai, bet ne rečiau kaip kartą per kalendorinius metus, peržiūri ir suderinęs su Užimtumo tarnybos direktoriumi patvirtina leistinos programinės įrangos sąrašą (standartinės ir papildomos programinės įrangos);

31.3. Įstaigos IS naudotojų kompiuterinėse darbo vietose ir tarnybinėse stotyse negali būti naudojama programinė įranga, nesusijusi su IS naudotojų funkcijų vykdymu. Standartinė programinė įranga Įstaigos IS naudotojų kompiuterinėse darbo vietose diegiama pagal nutylėjimą, rengiant kompiuterinę darbo vietą darbuotojui. Papildoma programinė įranga gali būti diegiama, jei ji būtina darbuotojo funkcijų vykdymui. Įranga, kuri nėra įtraukta į leistinos standartinės arba papildomos programinės įrangos sąrašą, tačiau ji reikalinga darbuotojo darbinių funkcijų vykdymui, gali būti diegiama tik suderinus su saugos įgaliotiniu ir įtraukus tokią įrangą į papildomos įrangos sąrašą;

31.4. programinę įrangą gali diegti tik administratorius (administratoriai), Įstaigos IS naudotojams draudžiama savavališkai diegti bet kokią programinę įrangą;

31.5. programinė įranga turi būti nuolat atnaujinama laikantis gamintojo reikalavimų. Įstaigos IS funkcionavimą užtikrinančios įrangos diegimą, priežiūrą, konfigūravimą, atnaujinimą, keitimą atsižvelgdami į gamintojų rekomendacijas atlieka Įstaigos IS administratoriai pagal priskirtas atitinkamas funkcijas;

31.6. periodiškai, bet ne rečiau kaip kartą per metus, turi būti atliekama naudojamos programinės įrangos patikrinimas, kurio metu tikrinama, ar Įstaigos IS naudotojų darbo vietose ir tarnybinėse stotyse nėra naudojama nelegali ar neleistina (neįtraukta į standartinės ir papildomos programinės įrangos sąrašus) programinė įranga. Rasta nelegali ar neleistina naudoti programinė įranga turi būti nedelsiant pašalinta;

31.7. turi būti įdiegta prieigos prie Įstaigos IS elektroninės informacijos registravimo, teisių suteikimo ir slaptažodžių sistema;

31.8. turi būti įgyvendinta prievolė reguliariai ne rečiau kaip kas 60 kalendorinių dienų keisti slaptažodžius Įstaigos IS naudotojams ir ne rečiau kaip kas 30 kalendorinių dienų keisti slaptažodžius Įstaigos IS administratoriams;

32. Informacijos saugai ir jos pasiekiamumui užtikrinti automatiniu būdu reguliariai – kiekvieną darbo dieną, daromos IS duomenų ir informacijos atsarginės kopijos.

33. Atsarginės kopijos turi būti saugomos kitose patalpose nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota. Atsarginės kopijos saugomos 14 kalendorinių dienų.

34. Prireikus atkurti informaciją iš atsarginių kopijų, teisę atkurti informaciją turi tik Įstaigos IS administratorius ar jį pavaduojantis asmuo.

35. Ne rečiau kaip kartą per metus turi būti atliekamas atsarginių kopijų išbandymas siekiant įsitikinti, kad informacija gali būti sėkmingai atkurta.

36. Siekiant užtikrinti Įstaigos IS saugumą ir tinkamą jų veikimą, kaupiami ir ne rečiau kaip kartą per mėnesį analizuojami šie žurnaliniai įrašai (angl. *log files*):

36.1. Įstaigos IS elementų (įskaitant, bet neapsiribojant tarnybinių stočių, taikomosios programinės įrangos) įjungimas ir išjungimas ar perkrovimas;

36.2. Įstaigos IS naudotojų ir administratorių prisijungimai ir nesėkmingi bandymai prisijungti prie informacinių sistemų bei atsijungimas nuo informacinių sistemų;

36.3. įvykių data, tikslus laikas ir trukmė;

36.4. IS naudotojų ir administratorių vykdomi veiksmai Įstaigos IS (įskaitant, bet neapsiribojant duomenų įvedimas, peržiūra, keitimas, naikinimas ir kiti duomenų tvarkymo veiksmai);

36.5. audito funkcijos įjungimas ir išjungimas, audito įrašų trynimas, kūrimas ar keitimas;

36.6. laiko ir (ar) datos pakeitimai;

36.7. kiti saugai svarbūs įvykiai, vykstantys kompiuterinio tinklo įrangoje, saugos užtikrinimo programinėje įrangoje, tarnybinėse stotyse.

37. Žurnaliniuose įrašuose turi būti fiksuojamas:

37.1. veiksmą atlikusio Įstaigos IS naudotojo identifikatorius, įvykio data ir tikslus laikas;

37.2. įvykio rūšis / pobūdis;

37.3. Įstaigos IS naudotojo ir (arba) administratoriaus ir (arba) Įstaigos IS įrenginio, susijusio su įvykiu, duomenys;

37.4. įvykio rezultatas.

38. Žurnaliniai įrašai turi būti apsaugoti nuo galimybės juos ištrinti ar pakeisti.

39. Žurnaliniai įrašai turi būti kaupiami ir saugomi centralizuotai techninėje ar programinėje įrangoje, skirtoje audito duomenims saugoti, ir analizuojami Įstaigos IS administratoriaus ne rečiau kaip kartą per mėnesį. Apie analizės rezultatus turi būti informuojamas saugos įgaliotinis.

40. Žurnaliniai įrašai turi būti saugomi ne trumpiau kaip 60 dienų užtikrinant visas prasmingas jų turinio reikšmes. Draudžiama ištrinti žurnalinius įrašus kol nesibaigęs jų saugojimo terminas. Pasibaigus saugojimo terminui žurnaliniai įrašai gali būti archyvuojami. Audito duomenys turi būti prieinami tik saugos įgaliotiniui ir Įstaigos IS administratoriui (administratoriams) (peržiūros teisėmis).

41. Dėl įvairių trikdžių nustojus fiksuoti žurnalinius įrašus, apie tai nedelsiant, bet ne vėliau kaip per vieną darbo dieną, centralizuota techninė ar programinė įranga, skirta audito duomenims saugoti, turi informuoti Įstaigos IS administratorių (administratorius) ir saugos įgaliotinį.

42. Įvykus įtartinai veiklai, centralizuota techninė ar programinė įranga, skirta audito duomenims saugoti, turi užfiksuoti tai žurnaliniuose įrašuose ir sukurti pranešimą, kurį matytų Įstaigos IS administratorius (administratoriai). Toks pranešimas turi būti klasifikuojamas pagal užfiksuotą įvykį.

43. Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti fiksuojami ne vėliau kaip per dvidešimt keturias valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per septyniasdešimt dvi valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu Įstaigos IS valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio Įstaigos IS veiklai vertinimas (testavimas).

44. Pagrindinėse tarnybinėse stotyse turi būti įjungtos ugniasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su Įstaigos IS funkcionalumu ir administravimu susijusį duomenų srautą.

45. Įsilaužimo aptikimo konfigūracijos ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo Įstaigos IS techninės įrangos (kartu nurodant konfigūracijų ar taisyklių įgyvendinimo, atnaujinimo ir pan. datas, atsakingus asmenis, taikymo periodus ir panašiai).

46. Belaidžio tinklo saugumas ir kontrolė užtikrinama:

46.1. leidžiant naudoti tik su saugos įgaliotiniu suderintus belaidžio tinklo įrenginius,

atitinkančius techninius kibernetinio saugumo reikalavimus;

46.2. tikrinant eksploatuojamus belaidžius įrenginius ir saugos įgaliotiniui pranešant apie neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius;

46.3. belaidės prieigos taškus diegiant atskirame potinklyje, kontroliuojamoje zonoje;

46.4. prisijungiant prie belaidžio tinklo taikomas naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas;

46.5. belaidėje sąsajoje draudžiant naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą, taip pat draudžiami visi nereikalingi valdymo protokolai;

46.6. išjungiant nenaudojamus TCP (angl. *Transmission Control Protocol*) / UDP (angl. *User Datagram Protocol*) prievadus;

46.7. uždraudžiant lygiarangį (angl. *peer to peer*) funkcionalumą leidžiantį belaidžiais įrenginiais tarpusavyje palaikyti ryšį;

46.8. belaidį ryšį šifruojant mažiausiai 128 bitų ilgio raktu;

46.9. prieš pradedant šifruoti belaidį ryšį, turi būti pakeisti belaidės prieigos stotelėje standartiniai gamintojo raktai.

47. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių, neįskaitant mobiliųjų telefonų (toliau bendrai – mobilieji įrenginiai), naudojimo tvarka:

47.1. leidžiama naudoti tik su saugos įgaliotiniu suderintus mobiliuosius įrenginius, atitinkančius techninius kibernetinio saugumo reikalavimus. Jei darbuotojas nori naudoti savo mobilųjį įrenginį, jis turi atitikti nustatytus kibernetinio saugumo reikalavimus ir darbuotojas privalo sutikti su Įstaigos teise valdyti darbuotojo įrenginį (darbinę aplinką);

47.2. Įstaigos IS naudotojai yra atsakingi už jiems priskirtų mobilių įrenginių ir juose esančios informacijos apsaugą;

47.3. prieiga prie mobiliųjų įrenginių bei juose esanti informacija turi būti apsaugota naudotojo identifikatoriumi ir slaptažodžiu;

47.4. Įstaiga turi teisę valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą. Mobiliųjų įrenginių techninę ir programinę įrangą diegia ir prižiūri Įstaigos IS administratorius. Mobiliuosiuose įrenginiuose gali būti diegiama tik licencijuota programinė įranga;

47.5. turi būti tikrinami eksploatuojami mobilieji įrenginiai ir, nustačius neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius mobiliuosius įrenginius, informuojamas saugos įgaliotinis;

47.6. turi būti reguliariai įdiegiami operacinės sistemos ir kitos naudojamos programinės

įrangos gamintojų rekomenduojami atnaujinimai;

47.7. duomenys perduodami tarp mobiliojo įrenginio ir Įstaigos IS, turi būti šifruojami taikant virtualaus privataus tinklo (angl. *virtual private network, VPN*) technologiją;

47.8. mobilieji įrenginiai turi būti sukonfigūruoti, kad mobiliojo įrenginio naudotojas negalėtų atlikti mobiliojo įrenginio administratoriaus funkcijų, savarankiškai keisti mobiliojo įrenginio ar jame įdiegtos programinės įrangos nustatytų parametrų mobiliojo įrenginio darbo aplinkoje;

47.9. mobiliuosiuose įrenginiuose negali būti saugomi asmens duomenys ar kita svarbi informacija, išskyrus naudotojo darbo dokumentus. Mobiliuosiuose įrenginiuose saugoma informacija turi būti šifruojama. Šifravimui naudojamos operacinės sistemos priemonės arba naudojama specializuota programinė įranga, užtikrinanti reikiamą šifravimo patikimumo lygį. Mobiliuosiuose įrenginiuose esanti informacija turi būti šifruojama laikantis šių reikalavimų:

47.9.1. mobiliajame įrenginyje, kuriame saugomi jautrūs duomenys ar kurie gali būti naudojami prisijungimui prie Įstaigos IS, privalo būti įjungtas šifravimas;

47.9.2. informacijos šifravimui turi būti naudojamas ne mažesnis nei 128 bitų šifravimo standarto AES, RCA ar analogiškas algoritmas bei naudojamas saugus slaptažodis, sudarytas pagal Įstaigos slaptažodžių politiką;

47.9.3. šifravimo algoritmas ir šifravimo raktas turi būti saugomi atskirai skirtingose vietose;

47.10. Įstaigos IS administratorius ne rečiau kaip kartą per metus turi įvertinti šifravimo reikalavimų naudotojų mobiliuosiuose įrenginiuose atitikimo vertinimą.

48. Mobiliuosiuose įrenginiuose turi būti išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungtas lygiarangis (angl. *peer to peer*) funkcionalumas, belaidė periferinė prieiga.

49. Ne rečiau kaip kartą per mėnesį Įstaigos IS administratorius turi įvertinti kibernetiniam saugumui naudojamų priemonių programinius atnaujinimus, klaidų taisymus, kad būtų galima atnaujinti techninę ir programinę įrangą ir patikrinti jos nustatymus. Siekiant užtikrinti šių veiksmų atlikimą, naudotojai turi ne rečiau kaip kartą per mėnesį prisijungti prie Įstaigos kompiuterinio tinklo ar kitaip sudaryti sąlygas Įstaigos IS administratoriui atnaujinti programinę įrangą ir atlikti kitą būtinąjį mobiliojo įrenginio tvarkymą.

50. Kibernetinių incidentų valdymas vykdomas vadovaujantis Nacionalinio kibernetinių incidentų valdymo plano, patvirtinto Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau

– Kibernetinių incidentų valdymo planas) nuostatomis.

51. Visi kibernetiniai incidentai, įvykę Įstaigos IS, registruojami ir valdomi bei šalinami Įstaigos turimomis techninėmis ir programinėmis priemonėmis.

52. Įvykus kibernetiniam incidentui, Įstaigos IS administratorius ar kitas už kibernetinių incidentų valdymą paskirtas atsakingas darbuotojas, turi pranešti Nacionaliniam kibernetinio saugumo centui (toliau – NKSC) ir, esant numatytiems pagrindams – Policijai bei Valstybinei duomenų apsaugos inspekcijai (toliau – VDAI). Apie įvykusį kibernetinį incidentą pranešama NKCS interneto svetainėje nurodytais kontaktais arba užpildant formą NKSC svetainėje Kibernetinių incidentų valdymo plane nustatytais terminais bei pateikiant jame nurodytą informaciją.

53. Įstaigos IS įprastinės veiklos atkūrimą įvykus kibernetiniam incidentui, dėl kurio sutriko arba neveikia bent viena Įstaigos valdoma IS (ar jos dalis), galinti turėti neigiamą įtaką Įstaigos funkcijų vykdymui, nustato Veiklos tęstinumo valdymo planas. Įstaigos IS veiklos sutrikimas turi neviršyti maksimalus leistino paslaugos neveikimo laiko, nustatyto rizikos vertinimo metu atsižvelgiant į konkrečių informacinių sistemų svarbą bei galimą neigiamą poveikį Įstaigai bei kitiems susijusiems asmenims ir paslaugų gavėjams ir yra pateikiamas Saugos nuostatų 1 priede.

54. Kibernetinių incidentų valdymo patirtis įgyjama analizuojant ir vertinant įvykusius incidentus bei jų šalinimo metu įgytą patirtį, dalyvaujant kibernetinio saugumo nacionalinėse pratybose, o kibernetinio saugumo būklės gerinimas užtikrinamas dalyvaujant įvairiuose kibernetinio saugumo mokymuose.

55. Įstaigoje turi būti užtikrinamas dubliuotas ryšio ir interneto paslaugų teikimas.

56. Interneto paslaugų tiekėjams turi būti nustatomi minimalūs reikalavimai įtraukiant į sutartis:

56.1. reagavimo į kibernetinius incidentus įprastomis Įstaigos darbo valandomis ir po darbo valandų;

56.2. nepertraukiamo interneto paslaugos teikimo užtikrinimo dvidešimt keturias valandas per parą, septynias dienas per savaitę (24/7);

56.3. interneto paslaugos sutrikimų registravimo dvidešimt keturias valandas per parą, septynias dienas per savaitę (24/7);

56.4. apsaugos nuo Įstaigos IS trikdymo taikymo (angl. *Denial of Service, DoS*).

57. Elektroninio pašto naudojimo Įstaigoje sąlygos:

57.1. Įstaigos darbuotojams, Naudotojų administravimo taisyklėse nustatyta tvarka

suteikiant standartinį prieigos teisių rinkinį, yra sukuriama elektroninio pašto dėžutė ir suteikiamas elektroninio pašto adresas;

57.2. elektroninio pašto informacijai saugoti, darbuotojui skiriama nustatyto dydžio elektroninio pašto tarnybinės stoties disko talpa. Viršijus skirtą dydį, sistema apie tai informuoja naudotoją;

57.3. jei darbuotojo funkcijoms vykdyti yra būtina didesnė elektroninio pašto dėžutės talpa, struktūrinio padalinio vadovas teikia motyvuotą prašymą Kompiuterių techninės ir programinės įrangos gedimų ir informacinių sistemų bei kitų su informacinėmis technologijomis susijusių problemų registravimo tvarkos apraše, patvirtiname Užimtumo tarnybos direktoriaus 2021 m. gruodžio 9 d. įsakymu Nr. V-502 „Dėl kompiuterių techninės ir programinės įrangos gedimų ir informacinių sistemų bei kitų su informacinėmis technologijomis susijusių problemų registravimo tvarkos aprašo patvirtinimo“, nustatyta tvarka;

57.4. elektroniniu paštu siunčiamiems ir gaunamiems pranešimams nustatytas maksimalus 11 MB dydis. Viršijus nustatytą elektroninio pašto pranešimo dydį, sistema apie tai informuoja naudotoją;

57.5. elektroninis paštas turi būti naudojamas darbo reikmėms – visa darbinė informacija turi būti siunčiama tik naudojantis Įstaigos elektroniniu paštu;

57.6. elektroninio pašto naudotojai privalo laikytis saugaus elektroninio pašto naudojimosi reikalavimų bei užtikrinti siunčiamos informacijos konfidencialumą;

57.7. naudojantis elektroniniu paštu draudžiama:

57.7.1. savavališkai keisti elektroninio pašto programinės įrangos parametrus, susijusius su sauga arba prisijungimo būdu, ir kitus įdiegtus saugumo mechanizmus;

57.7.2. naudojantis elektroniniu paštu siųsti konfidencialią Įstaigos informaciją, įskaitant asmens duomenis, jei nenaudojamos papildomos informacijos saugos priemonės (pvz., siunčiamos informacijos šifravimas);

57.7.3. naudojantis elektroninio pašto paslauga siųsti pranešimus savo arba Įstaigos vardu, kurie gali pakenkti Įstaigos įvaizdžiui, sukelti materialinę arba moralinę žalą Įstaigai;

57.7.4. naudotis elektroniniu paštu sukčiavimo, reklamos ir asmeninės finansinės naudos tikslais;

57.7.5. kurti ar platinti laiškus su smurtinio, diskriminacinio, rasistinio, seksualinio ar kitaip žmogaus garbę ir orumą žeminančio turinio informaciją;

57.7.6. perduoti kitiems asmenims, įskaitant ir Įstaigos darbuotojus, elektroninio pašto prisijungimo vardus ir slaptažodžius ir naudotis svetimais elektroninio pašto adresais ir slaptažodžiais;

57.8. už elektroniniu paštu siunčiamos informacijos turinį ir saugumą atsako siuntėjas;

57.9. pasibaigus darbuotojo darbo santykiams, darbuotojo elektroninio pašto adresas naikinamas. Jei darbuotojo elektroninio pašto dėžutėje yra Įstaigos veiklai svarbios informacijos, ne vėliau kaip paskutinę darbuotojo darbo Įstaigoje dieną, atleidžiamas darbuotojas privalo perduoti tokią informaciją struktūrinio padalinio, kuriame jis dirbo, vadovui ar jo nurodytam darbuotojui. Jei ateityje į atleidžiamo darbuotojo elektroninio pašto dėžutę gali būti siunčiami elektroniniai laiškai, taip pat jei buvo vykdomas susirašinėjimas svarbiais Įstaigai klausimais, struktūrinio padalinio, kuriame dirbo darbuotojas, vadovas nedelsdamas informuoja elektroniniu paštu Infrastruktūros ir sistemų priežiūros skyrių dėl būtinumo nustatyti automatinį atsakymą, informuojantį siuntėją, kad elektroninio pašto adresas nebenaudojamas bei nurodant kitą Įstaigos darbuotoją, su kuriuo siuntėjas galėtų susisiekti.

58. Įstaigos interneto svetaines prižiūri atitinkamos Įstaigos IS ar posistemio tvarkytojas. Informacija interneto svetainėse turi būti tinkamai apsaugota. Prieigą prie interneto svetainių kontroliuoja ir techninę priežiūrą atlieka Įstaigos IS administratorius:

58.1. svetainės turi atitikti Kibernetinio saugumo reikalavimų aprašo nustatytus techninius reikalavimus;

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

58.3. turi būti pakeistos numatytos prisijungimo prie svetainių turinio valdymo sistemų ir administravimo skydų (angl. *Panel*) nuorodos (angl. *Default path*) ir slaptažodžiai;

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

59. Įstaigos IS turi būti įgyvendinti techniniai kibernetinio saugumo reikalavimai, atsižvelgiant į konkrečios informacinės sistemos kategoriją bei tokios kategorijos informacinėms sistemoms privalomus taikyti kibernetinio saugumo reikalavimus, kurie nustatyti 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“. Detalus privalomų taikyti reikalavimų sąrašas pateikiamas Saugos nuostatų 2 priede.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

60. Saugos įgaliotiniu negali būti asmuo, turintis neišnykusį ar nepanaikintą teistumą už nusikaltimus elektroninių duomenų ir informacinių sistemų saugumui, taip pat paskirtą administracinę nuobaudą už Kibernetinio saugumo įstatymo pažeidimus, susijusius su saugumo nustatytos informacijos teikimo pareigos neatlikimu ar paskirtą administracinę nuobaudą už neteisėtą asmens duomenų tvarkymą ir privatumo apsaugos pažeidimą elektroninių ryšių srityje, elektroninių ryšių išteklių naudojimo ir skyrimo taisyklių pažeidimą, elektroninių ryšių tinklo gadinimą ar savavališką prisijungimą prie tinklo arba galinių įrenginių, kurie trukdo elektroninių ryšių tinklo darbui, savavališką prisijungimą arba elektroninių ryšių infrastruktūros įrengimo, naudojimo ir apsaugos sąlygų ir taisyklių pažeidimą, jeigu nuo jos paskyrimo praėję mažiau kaip vieni metai.

61. Saugos įgaliotinis turi:

61.1. išmanyti elektroninės informacijos saugos ir kibernetinio saugumo užtikrinimo principus;

61.2. šiuolaikinių informacinių technologijų naudojimo ypatumus, būti susipažinęs su informacijos saugą ir kibernetinį saugumą užtikrinančiais technologiniais sprendimais bei jų veikimo principais;

61.3. būti susipažinęs su informacijos saugos rizikos vertinimo metodikomis, sugebėti vertinti rizikos veiksnių tikimybes ir žalos galimybes, organizuoti ir kontroliuoti trūkumų šalinimą;

61.4. privalo reguliariai kelti savo kvalifikaciją;

61.5. vykdydamas jam priskirtas funkcijas, vadovautis Saugos nuostatais ir saugos dokumentais ir kitų Užimtumo tarnybos teisės aktų bei Lietuvos Respublikos ir Europos Sąjungos teisės aktų nuostatomis, reglamentuojančiomis elektroninės informacijos saugą ir kibernetinį saugumą.

62. Įstaigos IS administratorius, atsižvelgiant į vykdomas funkcijas, turi:

62.1. išmanyti darbą su kompiuterių tinklais ir mokėti užtikrinti jų saugumą;

62.2. mokėti administruoti ir prižiūrėti duomenų bazes;

62.3. būti susipažinęs su šiais Saugos nuostatais bei kitais Saugos dokumentais ir kitais Lietuvos Respublikos ir Europos Sąjungos teisės aktais, reglamentuojančiais elektroninės informacijos saugą ir kibernetinį saugumą bei saugų elektroninės informacijos tvarkymą.

63. Įstaigos IS naudotojai, vadovaudamiesi Saugos nuostatais ir kitais Saugos dokumentais, pareigybių aprašymais ir kitais teisės aktais, naudoja Įstaigos IS informaciją informacijos tvarkymo arba kitais su darbo funkcijų vykdymu susijusiais tikslais.

64. Įstaigos IS naudotojams gali būti suteikiamos tik tokios prieigos teisės, kurios būtinos jų darbo funkcijų vykdymui. Įstaigos IS naudotojams negali būti suteikiamos Įstaigos IS administratoriaus teisės. Bet koks Įstaigos IS administratoriaus teisių Įstaigos IS naudotojams suteikimas turi būti suderintas su saugos įgaliotiniu ir įvertinta tokių teisių suteikimo rizika bei numatytos rizikos mažinimo priemonės.

65. Tvarkyti Įstaigos IS informaciją ir ją naudoti gali tik įgalioti Įstaigos IS naudotojai, susipažinę su Saugos dokumentais ir raštu sutikę laikytis juose nustatytų reikalavimų. Už Įstaigos IS naudotojų supažindinimą su saugos dokumentais, atsakingas saugos įgaliotinis. Naudotojų supažindinimą su Saugos dokumentais Saugos įgaliotinis organizuoja per Dokumentų valdymo sistemą ar kitu priimtinu būdu, kad būtų užtikrintas susipažinimo įrodomumas. Saugos įgaliotinis informuoja IS naudotojus apie Saugos dokumentų priėmimą, pakeitimą ar pripažinimą netekusiais galios, pakeitus Saugos dokumentus naudotojai privalo iš naujo susipažinti su jais.

66. Įstaigos IS naudotojai privalo turėti darbo su kompiuteriu įgūdžių, mokėti tvarkyti Įstaigos IS duomenis konkrečios informacinės sistemos nuostatų nustatyta tvarka.

67. Susipažinti su Įstaigos IS saugoma elektronine informacija ir ją tvarkyti gali tik tie Įstaigos IS naudotojai, kuriems Informacinių sistemų naudotojų administravimo taisyklėse nustatyta tvarka buvo suteiktos prieigos prie Įstaigos IS ir informacijos teisės.

68. Kiekvienas Įstaigos IS naudotojas konkrečiose informacinėse sistemose turi būti identifikuojamas unikaliai (asmens kodas negali būti naudojamas kaip naudotojo identifikatorius). Draudžiama naudoti bendras paskyras, išskyrus jei tai būtina Įstaigos veiklos procesams užtikrinti ir nėra kitų galimybių. Bendrų paskyrų naudojimas turi būti suderintas su saugos įgaliotiniu ir įvertinta tokių bendrų paskyrų naudojimo rizika bei numatytos rizikos mažinimo priemonės.

69. Įstaigos IS naudotojai privalo nedelsdami pranešti apie Įstaigos IS ar jų posistemių veiklos sutrikimus, esamus arba įtariamus, kibernetiniu incidentus, Saugos nuostatuose ir Saugos dokumentuose nustatytų reikalavimų pažeidimus, neveikiančias arba netinkamai veikiančias saugos priemones, kitų naudotojų ar asmenų neteisėtus veiksmus ar nusikalstamos veikos požymius turinčius atvejus ar kitus įtartinus atvejus Įstaigos IS administratoriui ir (arba) saugos įgaliotiniui.

70. Įstaigos IS naudotojai turi kelti savo kvalifikaciją informacijos saugos ir kibernetinio saugumo srityje, kasmet dalyvauti Įstaigos mokymų plane suplanuotuose ir (arba) saugos įgaliotinio organizuojamuose mokymuose informacijos saugos ir kibernetinio saugumo klausimais bei pasiekti numatytus rezultatus, susipažinti su saugos įgaliotinio pateikiama informacija apie aktualias kibernetines grėsmes ar problemas.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

71. Saugos nuostatai turi būti peržiūrimi ir, jei reikia, atnaujinami, ne rečiau kaip kartą per metus, taip pat įvykus esminiams organizaciniams, sisteminiams ar kitiems Įstaigos pokyčiams ar įvykus pavojingo ar didelio poveikio kibernetiniams incidentams.

72. Asmenys, pažeidę Saugos nuostatų reikalavimus, atsako teisės aktų nustatyta tvarka.

_____

Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų duomenų saugos nuostatų
1 priedas

UŽIMTUMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS VALDOMŲ INFORMACINIŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	**Informacinė sistema**	**Informacinės sistemos paskirtis**	**Informacinės sistemos savininkas**	**Informacinės sistemos elektroninės informacijos svarbos kategorija ir priskyrimo kriterijai**	**Informacinės sistemos kategorija**	**Maksimalus leistinas IS neveikimo laikas**
1	Lietuvos darbo biržos informacinė sistema (LDB IS, eDBirža)	IT priemonėmis valdyti šalies darbo rinkos stebėseną, fiziniams ir juridiniams asmenims teikiamas darbo rinkos, profesinės reabilitacijos ir administracines paslaugas bei taikomas užimtumo rėmimo priemones ir Lietuvos Respublikos valstybės įmonės Ignalinos atominės elektrinės darbuotojams papildomas užimtumo ir socialines garantijas, taip pat sudaryti sąlygas struktūrizuotų elektroninių dokumentų	Užimtumo tarnyba	Svarbi informacija: 8.1. sudaryti sąlygas kilti pavojui žmogaus gyvybei arba sukelti pavojų žmogaus sveikatai ar kitaip pažeisti daugiau kaip 5 procentų, bet ne daugiau nei pusės valstybės gyventojų kitas teises ir teisėtus interesus; 8.2. lemti, kad nebus atliekama (-os) kuri nors (kurios nors) gyvybiškai svarbi (-ios) funkcija (-os) daugiau nei vienam ministrui pavestose valdymo srityse; 8.3. vienai ar kelioms institucijoms padaryti finansinių nuostolių, didesnių	2	12 val.

Eil. Nr.	Informacinė sistema	Informacinės sistemos paskirtis	Informacinės sistemos savininkas	Informacinės sistemos elektroninės informacijos svarbos kategorija ir priskyrimo kriterijai	Informacinės sistemos kategorija	Maksimalus leistinas IS neveikimo laikas
		apsikeitimui tarp valstybių narių kompetentingų įstaigų per elektroninių socialinės apsaugos informacijos mainų sistemą (EESSI sistema)		nei 300 000 eurų, bet ne didesnių nei 3 000 000 eurų; 8.4. padaryti žalą aplinkai daugiau nei vienoje, bet ne daugiau nei 5 apskrityse; 8.5. sukelti grėsmę viešajam saugumui daugiau nei vienoje, bet ne daugiau nei 5 apskrityse; 8.6. sukelti tarptautinių sutarčių ir įsipareigojimų pažeidimą, kurio padarinių šalinimo nuostoliai būtų didesni nei 300 000 eurų, bet ne didesni nei 3 000 000 eurų.		
2	***Neteko galios nuo 2023-12-22***				2	12 val.
3	Personalo valdymo informacinė sistema (PVS, Bonus)	Personalo ir darbo užmokesčio sistema	Užimtumo tarnyba	Mažiausios svarbos informacija	4	24 val.
4	DocLogix (DVS)	Dokumentų valdymo sistema	Užimtumo tarnyba	Mažiausios svarbos informacija	4	24 val.
5	Interneto svetainės	Skelbti informaciją apie Užimtumo tarnybos funkcijas, struktūrą, veiklą. Skatinti asmenis aktyviai dalyvauti valstybės valdymo ar vietos savivaldos procese.	Užimtumo tarnyba	Mažiausios svarbos informacija	4	24 val.

Eil. Nr.	Informacinė sistema	Informacinės sistemos paskirtis	Informacinės sistemos savininkas	Informacinės sistemos elektroninės informacijos svarbos kategorija ir priskyrimo kriterijai	Informacinės sistemos kategorija	Maksimalus leistinas IS neveikimo laikas
		Užtikrinti Užimtumo tarnybos veiklos skaidrumą. Teikti viešąsias ir (arba) administracines paslaugas elektroninių ryšių priemonėmis.				

_____

Užimtumo tarnybos prie Lietuvos Respublikos
socialinės apsaugos ir darbo ministerijos
informacinių sistemų duomenų saugos nuostatų
2 priedas

TECHNINIŲ KIBERNETINIO SAUGUMO REIKALAVIMŲ SĄRAŠAS

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
		II kat.[1]	IV kat.[2]
1 lentelė. Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumas ir kontrolė			
1.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros priežiūrą vykdančio asmens (toliau – administratorius) funkcijos turi būti atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo funkcijoms atlikti	x	x
2.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojams negali būti suteikiamos administratoriaus teisės	x	x
3.	Kiekvienas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas turi būti unikaliai atpažįstamas (asmens kodas negali būti naudojamas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui atpažinti)	x	x
4.	Viešaisiais elektroninių ryšių tinklais perduodamos informacijos konfidencialumas turi būti užtikrintas naudojant šifravimą, virtualųjį privatų tinklą (angl. *Virtual private network, VPN*)	x	x
5.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone	x	x
6.	Administratorių tapatumui patvirtinti turi būti naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	

[1] Reikalavimai, privalomi LDB IS ir SIDA
[2] Reikalavimai, privalomi PVS, DVS, interneto svetainėms

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
7.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo teisė dirbti su konkrečiu valstybės informaciniu ištekliumi ar ypatingos svarbos informacine infrastruktūra turi būti sustabdoma, kai valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas nesinaudoja valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra ilgiau kaip tris mėnesius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x
8.	Administratoriaus teisė dirbti su valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra turi būti sustabdoma, kai administratorius nesinaudoja valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra ilgiau kaip du mėnesius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x
9.	Kai įstatymų nustatytais atvejais valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas ar administratorius nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo ar administratoriaus kvalifikacinių reikalavimų, taip pat pasibaigia jo darbo (tarnybos) santykiai, jis praranda patikimumą, jo teisė naudotis valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra turi būti panaikinta nedelsiant	x	x
10.	Nereikalingos ar nenaudojamos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų ir administratoriaus paskyros turi būti blokuojamos nedelsiant ir ištrinamos praėjus audito duomenų nustatytam saugojimo terminui	x	x
11.	Baigus darbą arba valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui pasitraukiant iš darbo vietos, turi būti imamasi priemonių, kad su informacija, kuri tvarkoma valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje, negalėtų susipažinti pašaliniai asmenys: turi būti atsijungiama nuo valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, įjungiama ekrano užsklanda su slaptažodžiu (jeigu valstybės informacinių išteklių ar ypatingos svarbos	x	x

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
	informacinės infrastruktūros dalys palaiko tokį funkcionalumą)		
12.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje neatliekant jokių veiksmų, darbo stotis turi užsirakinti, kad toliau naudotis valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra būtų galima tik pakartotinai patvirtinus savo tapatybę (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą). Laikas, per kurį valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui neatliekant jokių veiksmų darbo stotis užsirakina, nustatomas kibernetinio saugumo politikos ir jos įgyvendinimo dokumentuose, tačiau negali būti ilgesnis kaip penkiolika minučių. Šis reikalavimas netaikomas, jeigu, atlikus ryšių ir informacinių sistemų rizikos vertinimą, nustatomos kitos nustatytą riziką atitinkančios techninės kibernetinio saugumo priemonės	x	x
13.	Prisijungimo prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros slaptažodžių reikalavimai:	x	x
13.1.	Slaptažodis turi būti sudarytas iš raidžių, skaičių ir specialiųjų simbolių	x	x
13.2.	Slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai)	x	x
13.3.	Draudžiama slaptažodžius atskleisti kitiems asmenims	x	x
13.4.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys, patvirtinančios valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo tapatumą, turi drausti išsaugoti slaptažodžius (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
13.5.	Turi būti nustatytas didžiausias leistinas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo mėginimų įvesti teisingą slaptažodį skaičius (ne daugiau kaip penki kartai) (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą). Iš eilės neteisingai įvedus slaptažodį tiek kartų, kiek nustatyta, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo paskyra turi užsirakinti ir neleisti valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui patvirtinti tapatybės kibernetinio saugumo politikos ir jos įgyvendinimo dokumentuose nustatytą laiką – ne trumpiau kaip penkiolika minučių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x
13.6.	Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą, sprendimu tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu	x	x
13.7.	Papildomi valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo slaptažodžių reikalavimai:		
13.7.1.	Slaptažodis turi būti keičiamas ne rečiau kaip kas tris mėnesius	x	
13.7.2.	Slaptažodį turi sudaryti ne mažiau kaip aštuoni simboliai (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	
13.7.3.	Keičiant slaptažodį, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros neturi leisti sudaryti slaptažodžio iš buvusių šešių paskutinių slaptažodžių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
13.7.4.	Pirmąkart jungiantis prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, turi būti reikalaujama, kad valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojas pakeistų slaptažodį (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x
13.8.	Papildomi administratorių slaptažodžių reikalavimai:	x	x
13.8.2.	Slaptažodis turi būti keičiamas ne rečiau kaip kas du mėnesius	x	
13.8.3.	Slaptažodį turi sudaryti ne mažiau kaip dvylika simbolių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	
13.8.4.	Keičiant slaptažodį, taikomoji programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių trijų paskutinių slaptažodžių (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	
14.	Turi būti patvirtinti asmenų, kuriems suteiktos administratoriaus teisės prisijungti prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, sąrašai, periodiškai peržiūrimi kompetentingo asmens ar padalinio, atsakingo už kibernetinio saugumo organizavimą ir užtikrinimą. Sąrašas turi būti nedelsiant peržiūrėtas, kai įstatymų nustatytais atvejais administratorius nušalinamas nuo darbo (pareigų)	x	
15.	Turi būti vykdoma administratorių paskyrų kontrolė:	x	x
15.1.	Periodiškai tikrinama, ar nėra nepatvirtintų administratoriaus paskyrų		x
15.2.	Naudojamos administratorių paskyrų kontrolės priemonės, kurios tikrina administratoriaus paskyras. Apie nepatvirtintas administratoriaus paskyras turi būti pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą	x	
16.	Vykdoma valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyrų kontrolė:		

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
16.1.	Tikrinama, ar nėra nepatvirtintų valstybės informacinių išteklių arba ypatingos svarbos informacinės infrastruktūros naudotojų paskyrų, ir pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, apie nepatvirtintas valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyras	x	x
16.2.	Naudojamos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyrų kontrolės priemonės, kurios periodiškai tikrina valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų paskyras. Apie nepatvirtintas paskyras turi būti pranešama kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą	x	
17.	Draudžiama valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros techninėje ir programinėje įrangoje naudoti gamintojo nustatytus slaptažodžius, jie turi būti pakeisti į atitinkančius reikalavimus	x	x
2 lentelė. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, jos naudotojų ir administratorių atliekamų veiksmų auditas ir kontrolė			
18.	Auditui atlikti turi būti fiksuojama ši informacija:		
18.1.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros elementų įjungimas / išjungimas ar perkrovimas (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	x
18.2.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti) / atsijungimas	x	x
18.3.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojų / administratorių teisių naudotis sistemos / tinklo ištekliais pakeitimai (jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros dalys palaiko tokį funkcionalumą)	x	
18.4.	Audito funkcijos įjungimas / išjungimas	x	x
18.5.	Audito įrašų trynimas, kūrimas ar keitimas	x	x
18.6.	Laiko ir (ar) datos pakeitimai	x	
19.	Audituojamų įrašų laiko žymos turi būti sinchronizuotos ne mažiau kaip vienos sekundės tikslumu	x	
20.	Kiekviename audito duomenų įraše turi būti fiksuojama:		

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
20.1.	Įvykio data ir tikslus laikas	x	x
20.2.	Įvykio rūšis / pobūdis	x	
20.3.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo / administratoriaus ir (arba) valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros įrenginio, susijusio su įvykiu, duomenys	x	x
20.4.	Įvykio rezultatas	x	x
21.	Priemonės, naudojamos valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais	x	
22.	Valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje fiksuojami įvykiai turi būti saugomi techninėje ar programinėje įrangoje, pritaikytoje audito duomenims saugoti	x	
23.	Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant, bet ne vėliau kaip vieną darbo dieną turi būti informuojamas administratorius ir kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	x	
24.	Audito duomenys turi būti saugomi ne trumpiau kaip šešiasdešimt dienų, užtikrinant visas prasmingas jų turinio reikšmes (pavyzdžiui, valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudotojo, su kuriuo nutraukti darbo santykiai ir kuris pašalintas iš sistemos, atpažinties duomenys turi būti išsaugoti visą būtiną audito duomenų saugojimo laiką)	x	
25.	Draudžiama audito duomenis trinti, keisti, kol nesibaigęs audito duomenų saugojimo terminas	x	x
26.	Audito duomenų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo	x	
27.	Naudojimasis audito duomenimis turi būti kontroliuojamas ir fiksuojamas. Audito duomenys turi būti pasiekiami tik administratoriui ir kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą (peržiūros teisėmis)	x	
28.	Audito įrašų duomenys turi būti analizuojami administratoriaus ne rečiau kaip kartą per mėnesį ir apie analizės rezultatus informuojamas kompetentingas asmuo ar padalinys, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą	x	
3 lentelė. Įsibrovimų aptikimas ir prevencija			

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
29.	Turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų	x	x
30.	Įvykus įtartinai veiklai, tai turi būti užfiksuojama audito įrašuose ir kuriamas pranešimas, kurį matytų administratorius	x	
31.	Sukurtas pranešimas turi būti klasifikuojamas pagal užfiksuotą įvykį	x	
32.	Įsilaužimo atakų požymiai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų požymiai turi būti įdiegiami ne vėliau kaip per dvidešimt keturias valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų požymių datos arba ne vėliau kaip per septyniasdešimt dvi valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų požymius datos, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo sprendimu atliekamas įsilaužimo atakų požymių įdiegimo ir galimo jų poveikio valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros veiklai vertinimas (testavimas)	x	
33.	Pagrindinėse tarnybinėse stotyse turi būti įjungtos saugasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį, išskyrus su valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros funkcionalumu ir administravimu susijusį duomenų srautą	x	x
34.	Įsilaužimo aptikimo konfigūracijos ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros techninės įrangos (kartu nurodant atitinkamas datas (įgyvendinimo, atnaujinimo ir panašiai), atsakingus asmenis, taikymo periodus ir panašiai)	x	x
4 lentelė. Belaidžio tinklo saugumas ir kontrolė			
35.	Leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidžio tinklo įrenginius, atitinkančius techninius kibernetinio saugumo reikalavimus	x	x
36.	Turi būti vykdoma belaidžių įrenginių kontrolė:	x	x

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
36.1.	Tikrinami valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje eksploatuojami belaidžiai įrenginiai, kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, pranešama apie neleistinus ar techninių kibernetinio saugumo reikalavimų neatitinkančius belaidžius įrenginius	x	x
36.2.	Naudojamos priemonės, kurios apribotų neleistinus ar saugumo reikalavimų neatitinkančius belaidžius įrenginius arba informuotų kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą	x	
36.3.	Leidžiama naudoti tik su kompetentingu asmeniu ar padaliniu, atsakingu už kibernetinio saugumo organizavimą ir užtikrinimą, suderintus belaidės prieigos taškus	x	x
37.	Belaidės prieigos taškai gali būti diegiami tik atskirame potinklyje, kontroliuojamoje zonoje	x	x
38.	Prisijungiant prie belaidžio tinklo, turi būti taikomas ryšių ir informacinių sistemų naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas	x	x
39.	Turi būti uždrausta belaidėje sąsajoje naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą	x	x
40.	Turi būti uždrausti visi nebūtini valdymo protokolai	x	x
41.	Turi būti išjungti nenaudojami TCP (angl. *Transmission Control Protocol*) / UDP (angl. *User Datagram Protocol*) prievadai	x	x
42.	Turi būti uždraustas lygiarangis (angl. *peer to peer*) funkcionalumas, neleidžiantis belaidžiais įrenginiais palaikyti ryšį tarpusavyje	x	x
43.	Belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu	x	x
44.	Prieš pradedant šifruoti belaidį ryšį, turi būti pakeisti belaidės prieigos stotelėje standartiniai gamintojo raktai	x	
45.	Kompiuteriuose, mobiliuosiuose įrenginiuose turi būti išjungta belaidė prieiga, jeigu jos nereikia darbo funkcijoms atlikti, išjungtas lygiarangis (angl. *peer to peer*) funkcionalumas, belaidė periferinė prieiga	x	
5 lentelė. Mobiliųjų įrenginių, naudojamų prisijungti prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, saugumas ir kontrolė			
46.	Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumo ir kontrolės reikalavimai, nurodyti šio priedo 1 lentelėje, taikytini pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros	x	x

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
	svarbos kategoriją		
47.	Leidžiama naudoti tik mobiliuosius įrenginius, atitinkančius valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo nustatytus saugumo reikalavimus	x	x
48.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojas turi turėti teises valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą	x	
49.	Turi būti vykdoma mobiliųjų įrenginių kontrolė:	x	x
49.1.	Tikrinami valstybės informaciniuose ištekliuose ar ypatingos svarbos informacinėje infrastruktūroje naudojami mobilieji įrenginiai, kompetentingam asmeniui ar padaliniui, atsakingam už kibernetinio saugumo organizavimą ir užtikrinimą, pranešama apie neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius	x	x
49.2.	Naudojamos priemonės, kurios apribotų neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius ar kompetentingą asmenį ar padalinį, atsakingą už kibernetinio saugumo organizavimą ir užtikrinimą, informuotų apie neleistinos mobiliosios įrangos prijungimą prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros	x	
50.	Turi būti įdiegiamos operacinės sistemos ir kiti naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai	x	x
51.	Turi būti parengti mobiliųjų įrenginių operacinių sistemų atvaizdai su saugumo nuostatomis. Atvaizde turi būti nustatyti tik veiklai būtini operacinių sistemų komponentai (administravimo paskyros, paslaugos (angl. *Services*), taikomosios programos, tinklo prievadai, atnaujinimai, sisteminės priemonės). Atvaizdai turi būti reguliariai peržiūrimi ir atnaujinami, iškart atnaujinami nustačius naujų pažeidžiamumų ar atakų	x	
52.	Pagal parengtus atvaizdus į mobiliuosius įrenginius turi būti įdiegiama operacinė sistema su saugumo nuostatomis	x	
53.	Mobilieji įrenginiai, kuriais naršoma internete, turi būti apsaugoti nuo judriųjų programų (angl. *Mobile code*) keliamų grėsmių	x	
54.	Prie mobiliųjų įrenginių draudžiama prijungti jiems nepriklausančius įrenginius	x	

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
55.	Duomenys, perduodami tarp mobiliojo įrenginio ir valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, turi būti šifruojami taikant virtualaus privataus tinklo (angl. *VPN*) technologiją	x	
56.	Jungiantis prie valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, turi būti patvirtinamas tapatumas; mobiliajame įrenginyje ar jo taikomojoje programinėje įrangoje turi būti uždrausta išsaugoti slaptažodį	x	
57.	Nešiojamasis prietaisas, gaunantis energiją iš integruoto energijos šaltinio ir turintis galimybę perduoti ir (ar) priimti ir apdoroti elektroninius duomenis, siunčiamus fizine terpe, elektromagnetinėmis bangomis ir šviesa, kuriuo nesinaudojama nustatytą laiką (pavyzdžiui, penkias minutes), turi automatiškai užsirakinti	x	
58.	Turi būti užtikrinta kompiuterinių laikmenų apsauga	x	x
59.	Turi būti šifruojami duomenys ir mobiliųjų įrenginių laikmenose, ir išorinėse kompiuterinėse laikmenose	x	
6 lentelė. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamos interneto svetainės, pasiekiamos iš viešųjų elektroninių ryšių tinklų, saugumas ir kontrolė			
60.	Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumo ir kontrolės reikalavimai, nurodyti šio priedo skyriuje „Atpažinties, tapatumo patvirtinimo ir naudojimosi valstybės informaciniais ištekliais ar ypatingos svarbos informacine infrastruktūra saugumas ir kontrolė“, taikytini pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbos kategoriją	x	x
61.	Papildomi atpažinties, tapatumo patvirtinimo ir naudojimosi kontrolės reikalavimai:		
61.1.	Draudžiama slaptažodžius saugoti programiniame kode	x	x
61.2.	Svetainės, patvirtinančios nuotolinio prisijungimo tapatumą, turi drausti išsaugoti slaptažodžius	x	
62.	Turi būti įgyvendinti svetainės kriptografijos reikalavimai:		
62.1.	Atliekant svetainės administravimo darbus ryšys turi būti šifruojamas naudojant ne trumpesnį kaip 128 bitų raktą	x	x
62.2.	Šifruojant naudojami skaitmeniniai sertifikatai privalo būti išduoti patikimų sertifikavimo tarnybų. Sertifikato raktas turi būti ne trumpesnis kaip 2048 bitų	x	
62.3.	Turi būti naudojamas TLS (angl. *Transport Layer Security*) standartas	x	

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
62.4.	Svetainės kriptografinės funkcijos turi būti įdiegtos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. *Hardware security module*)	x	
62.5.	Visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. *fail securely*)	x	
62.6.	Kriptografiniai raktai ir algoritmai turi būti valdomi pagal ryšių ir informacinių sistemų valdytojo reikalavimus	x	x
63.	Tarnybinės stoties, kurioje yra svetainė, svetainės saugos parametrai turi būti teigiamai įvertinti naudojant Nacionalinio kibernetinio saugumo centro rekomenduojamą testavimo priemonę	x	
64.	Draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai	x	x
65.	Turi būti naudojama svetainės saugasienė (angl. *Web Application Firewall*). Įsilaužimo atakų požymiai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų požymiai turi būti įdiegiami ne vėliau kaip per dvidešimt keturias valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per septyniasdešimt dvi valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų požymius datos, jeigu valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojo sprendimu atliekamas įsilaužimo atakų požymių įdiegimo ir galimo jų poveikio valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros veiklai vertinimas (testavimas)	x	
66.	Turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: struktūrizuotų užklausų kalbos įskverbties (angl. *SQL injection*), įterptinių instrukcijų atakų (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), paskirstyto atsisakymo aptarnauti (angl. *DDOS*) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)*) interneto svetainėje www.owasp.org	x	
67.	Turi būti naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė (angl. *Validation*)	x	
68.	Tarnybinė stotis, kurioje yra svetainė, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį	x	

Eil. Nr.	Reikalavimai	Informacinės sistemos kategorija	
69.	Svetainės saugumo priemonės turi gebėti uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai)	x	
70.	Atliekamų veiksmų audito ir kontrolės reikalavimai, nurodyti šio priedo skyriuje „Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros, jos naudotojų ir administratorių atliekamų veiksmų auditas ir kontrolė“, taikytini pagal valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros svarbos kategoriją	x	x
71.	Tarnybinė stotis, kurioje yra svetainė, turi leisti tik svetainės funkcionalumui užtikrinti reikalingus protokolo (angl. *HTTP*) metodus	x	x
72.	Turi būti uždrausta naršyti svetainės aplankuose (angl. *Directory browsing*)	x	x
73.	Turi būti įdiegta svetainės turinio nesankcionuoto pakeitimo (angl. *Defacement*) stebėsenos sistema	x	
7 lentelė. Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros naudojamo interneto saugumas ir kontrolė			
74.	Valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros valdytojas su interneto paslaugos teikėju (-ais) turi būti sudaręs šias sutartis:	x	x
74.1.	Reagavimo į kibernetinius incidentus įprastomis darbo valandomis	x	x
74.2.	Reagavimo į kibernetinius incidentus po darbo valandų	x	
74.3.	Nepertraukiamo interneto paslaugos teikimo:	x	x
74.3.1.	įprastomis darbo valandomis		x
74.3.2.	dvidešimt keturias valandas per parą, septynias dienas per savaitę	x	
74.4.	Interneto paslaugos sutrikimų registravimo:	x	x
74.4.1.	įprastomis darbo valandomis		x
74.4.2.	dvidešimt keturias valandas per parą, septynias dienas per savaitę	x	
74.5.	Apsaugos nuo valstybės informacinių išteklių ar ypatingos svarbos informacinės infrastruktūros trikdymo taikymo (angl. *Denial of Service, DoS*)	x	x

---

Priedo pakeitimai:
Nr. V-252, 2023-12-21, paskelbta TAR 2023-12-21, i. k. 2023-24884

Priedo pakeitimai:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

1 priedas. *Neteko galios nuo 2022-09-28*
Priedo naikinimas:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

2 priedas. *Neteko galios nuo 2022-09-28*

Priedo naikinimas:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

PATVIRTINTA
Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus
2021 m. kovo 19 d. įsakymu Nr. V-113
(Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus 2022 m. rugsėjo 27 d. įsakymo Nr. V-298 redakcija)

UŽIMTUMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos (toliau – Užimtumo tarnyba, Įstaiga) saugaus elektroninės informacijos tvarkymo taisyklės (toliau – Taisyklės) reglamentuoja saugų elektroninės informacijos ir duomenų tvarkymą Užimtumo tarnybos informacinėse sistemose (toliau – Įstaigos IS), nustato pagrindinius saugaus elektroninės informacijos tvarkymo reikalavimus, technines ir kitas saugos priemones, skirtas elektroninės informacijos saugai užtikrinti, reikalavimus taikomus Įstaigos valstybės tarnautojams ir darbuotojams, dirbantiems pagal darbo sutartis (toliau bendrai – darbuotojai), ir kitiems asmenims, kurie tiesioginių funkcijų vykdymui naudoja Įstaigos IS ir reikalavimus keliamus trečiųjų asmenų teikiamoms paslaugoms.

2. Taisyklėse vartojamos sąvokos:

2.1. **Duomenų centras** – specializuotos patalpos, skirtos centrinių ir tinklo kompiuterių įrangai talpinti, kuriose įrengtos minėtos įrangos nuolatiniam veikimui bei saugai užtikrinti būtinos inžinerinės sistemos (vėdinimo ir kondicionavimo, nuolatinio elektros maitinimo, priešgaisrinės saugos ir įėjimo kontrolės sistemos);

2.2. **Aptarnaujantis personalas** – trečiosios šalies paslaugų teikėjo, su kuriuo Užimtumo tarnyba yra pasirašiusi ryšio, techninės ar programinės įrangos priežiūros ar kitą sutartį, atstovas ar atstovai, teikiantys ryšio, techninės ar programinės įrangos priežiūros paslaugas Įstaigai.

3. Kitos Taisyklėse vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme, Bendrųjų 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“, 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“, Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų apraše, patvirtintame 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“, Lietuvos Respublikos standartuose LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“ ir LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų duomenų saugos nuostatuose.

4. Šios taisyklės privalomos Įstaigos IS valdytojui ir tvarkytojams, saugos įgaliotiniui, Įstaigos IS naudotojams, Įstaigos IS administratoriams ir aptarnaujančiam personalui.

5. Įstaigos IS tvarkomos elektroninės informacijos (jos grupių) sąrašas nurodytas Taisyklių priede.

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

6. Saugiam elektroninės informacijos tvarkymui užtikrinti Užimtumo tarnyboje naudojamos kompiuterinės, sisteminės ir taikomosios programinės įrangos, fizinės, techninės ir organizacinės duomenų saugos priemonės:

6.1. Užimtumo tarnybos Infrastruktūros ir sistemų priežiūros skyrius nustato svarbiausią kompiuterinę techninę įrangą, duomenų perdavimo tinklo mazgus, ryšio linijas, reikalingas užtikrinti Įstaigos IS pasiekiamumą. Svarbiausia kompiuterinė techninė įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuojamos, jų techninė būklė nuolat stebima;

6.2. visai svarbiausiai programinei ir techninei įrangai (toliau – Įranga) turi būti teikiamas įrangos gamintojų arba jų atstovų garantinis aptarnavimas;

6.3. Įranga turi būti prižiūrima laikantis gamintojo instrukcijų ir rekomendacijų;

6.4. Įstaigos IS funkcionavimą užtikrinančios Įrangos diegimą, priežiūrą, atnaujinimą,

keitimą, atsižvelgdami į gamintojų instrukcijas ir rekomendacijas, atlieka Įstaigos IS administratoriai pagal priskirtas atitinkamas funkcijas arba aptarnaujantis personalas. Naudotojams yra draudžiama ardyti ar iškomplektuoti Įrangą ir jos sudedamąsias dalis ir (arba) keisti jų aparatinę sąranką;

6.5. Įranga ir elektroninės informacijos laikmenos turi būti laikomos taip, kad pašaliniai asmenys negalėtų prie jų prieiti, pasisavinti ar sugadinti. Visa Įranga yra registruojama ir apskaitoma, nurodoma kompiuterinės įrangos aparatinė sąranka ir naudotojai, kuriems priskirta įranga bei kasmet atliekama inventorizacija;

6.6. patalpose, kuriose yra Įstaigos IS tarnybinės stotys, turi būti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų pulto;

6.7. svarbiausios kompiuterinės įrangos darbas turi būti stebimas reguliariai. Įstaigos IS administratoriai turi būti perspėjami, kai pagrindinėje Įstaigos IS kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja;

6.8. naudotojų kompiuterinėse darbo vietose gali būti naudojamos tik darbo reikmėms skirtos išorinės duomenų laikmenos. Šios laikmenos negali būti naudojamos veiklai, nesusijusiai su teisėtu Įstaigos informacijos tvarkymu;

6.9. nuotolinė prieiga prie Įstaigos IS gali būti suteikiama tik tais atvejais, jei tai būtina darbuotojo tiesioginių funkcijų atlikimui. Nuotolinė prieiga galima tik naudojantis saugius šifruotus ryšio kanalus (*SSL VPN* tuneliu) arba naudojant sertifikatą. Savavališka nuotolinė prieiga prie Įstaigos informacinių sistemų yra griežtai draudžiama.

7. Sisteminės ir taikomosios programinės įrangos tarnybinių stočių ir naudotojų darbo vietų saugai užtikrinti naudojamos šios priemonės:

7.1. tarnybinėse stotyse ir darbuotojų kompiuterinėse darbo vietose naudojama tik legali ir licencijuota programinė įranga, reikalinga darbinių funkcijų vykdymui. Įstaigos Saugos įgaliotinis turi parengti, su Įstaigos direktoriumi suderinti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti leistinos programinės įrangos sąrašą;

7.2. turi būti operatyviai ištestuojami ir įdiegiami Įstaigos IS administratorių ir naudotojų darbo vietų kompiuterinės įrangos operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai. Įstaigos IS administratorius reguliariai, ne rečiau kaip kartą per savaitę, turi įvertinti informaciją apie Įstaigos IS, savarankiškoms sudedamosioms dalims, vidinių naudotojų darbo vietų kompiuterinei įrangai neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumų svarbos lygius;

7.3. tarnybinėse stotyse ir naudotojų kompiuterinėse darbo vietose apsaugai nuo virusų ir kitų kenkėjiškų programų turi būti įdiegtos centralizuotai valdoma ir atnaujinama kenksmingos

programinės įrangos aptikimo ir šalinimo priemonės (antivirusinė programinė įranga, nepageidaujamo elektroninio pašto valdymo įranga ir pan.). Šios priemonės turi automatiniu būdu informuoti administratorių apie tai, kurioms Įstaigos IS ar jų posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atnaujinimo laikas. Antivirusinės programinės įrangos kenksmingo kodo aprašai atnaujinami centralizuotai ne rečiau kaip kartą per darbo dieną;

7.4. kiekvienas Įstaigos IS naudotojas ir administratorius turi būti identifikuojamas unikaliai, draudžiama naudoti bendras paskyras išskyrus jei tai būtina Įstaigos veiklos procesams užtikrinti ir nėra kitų galimybių. Bendrų paskyrų naudojimas turi būti suderintas su Saugos įgaliotiniu ir įvertinta tokių bendrų paskyrų naudojimo rizika bei numatytos rizikos mažinimo priemonės;

7.5. programinę įrangą tarnybinėse stotyse ir kompiuterinėse darbo vietose turi teisę diegti tik Įstaigos IS administratoriai. Naudotojai neturi teisės be administratoriaus žinios diegti bet kokią programinę įrangą jiems priskirtose kompiuterinėse darbo vietose;

7.6. tarnybinių stočių operacinės sistemos turi būti konfigūruojamos laikantis gamintojo saugios konfigūracijos instrukcijų ir rekomendacijų;

7.7. visose kompiuterinėse darbo vietose turi būti nustatytas naudotojo prieigos blokavimas naudotojui 15 minučių neatliekant jokių veiksmų, prieiga prie kompiuterio leidžiama tik pakartotinai patvirtinus savo tapatybę. Naudotojas palikdamas kompiuterinę darbo vietą privalo imtis priemonių, kad su elektroninė informacija negalėtų susipažinti pašaliniai asmenys: atsijungti nuo informacinių sistemų arba įjungti slaptažodžiu apsaugotą kompiuterio ekrano užsklandą.

8. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

8.1. Įstaigos kompiuterinis tinklas įrengtas laikantis ne žemesnės nei UTP 5 kategorijos kompiuteriniams tinklams keliamų reikalavimų, tinklo kabeliai turi būti įmontuoti į specialius uždengtus lovelius;

8.2. Įstaigos kompiuterių tinklas turi būti segmentuotas atskiriant į atskirus potinklius tarnybinių stočių, Įstaigos IS naudotojų ir valdymo grupes. Planuojant ir pertvarkant kompiuterių tinklą turi būti numatomas vietinio tinklo segmentavimas, leidžiantis greitai ir nesunkiai keisti tinklo konfigūraciją įvykus incidentui;

8.3. Įstaigos IS elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų ryšių tinklų naudojant ugniasienes, įvykių žurnalai (angl. *log files*) turi būti reguliariai, tačiau ne rečiau kaip kartą per mėnesį analizuojami ir apie rezultatus pranešama Saugos įgaliotiniui, o saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

8.4. Įstaigos kompiuteriniame tinkle turi būti įdiegtos ir veikti automatizuotos įsibrovimo aptikimo sistemos, kurios stebėtų įeinantį ir išeinantį duomenų srautą ir vidinį srautą tarp

svarbiausių tinklo paslaugų;

8.5. pagrindinėse tarnybinėse stotyse turi būti įjungtos ugniasienės, sukonfigūruotos blokuoti visą įeinantį ir išeinantį duomenų srautą, išskyrus su informacinių sistemų funkcionalumu ir administravimu susijusį srautą. Ugniasienių konfigūracijų dokumentacija turi būti saugoma kartu su Įstaigos IS dokumentacija;

8.6. turi būti naudojamos ugniasienės, apsaugančios nuo pagrindinių per tinklą vykdomų atakų, kurių sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. *The Open Web Application Security Project (OWASP)*) interneto svetainėje www.owasp.org: SQL įskverbties (angl. *SQL injection*), XSS (angl. *Cross-site scripting*), atkirtimo nuo paslaugos (angl. *DOS*), dedikuoto atkirtimo nuo paslaugos (angl. *DDOS*) ir kitų;

8.7. pagrindinėse tarnybinėse stotyse turi būti naudojamos vykdomo kodo kontrolės priemonės, automatiškai apribojančios ar informuojančios apie neautorizuoto programinio kodo vykdymą;

8.8. Įstaigos tinklo perimetro apsaugai naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

8.9. viešaisiais ryšių tinklais perduodamos Įstaigos IS elektroninės informacijos konfidencialumas užtikrinamas naudojant šifravimą. Informacijos teikimas išoriniams gavėjams vykdomas naudojant saugų valstybinį duomenų perdavimo tinklą arba kitą saugų šifruotą duomenų perdavimo kanalą;

8.10. visos nenaudojamos Įstaigos kompiuterinio tinklo jungtys turi būti neaktyvios;

8.11. už saugų kompiuterių tinklo veikimą atsako Įstaigos IS administratorius arba aptarnaujantys darbuotojai.

9. Įstaigos patalpų ir aplinkos saugumo užtikrinimo priemonės:

9.1. įėjimas į Įstaigos patalpas yra kontroliuojamas apsaugos darbuotojų bei elektroninės įėjimo sistemos, į patalpas gali patekti tik Įstaigos darbuotojai ir asmenys, turintys leidimus;

9.2. Įstaigos patalpose ir teritorijoje, atsižvelgiant į asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimus, vykdomas vaizdo stebėjimas ir įrašymas;

9.3. Įstaigos patalpose įrengta apsauginė ir priešgaisrinė signalizacija (judesio ir dūžio bei dūmų ir temperatūros davikliai), perduodanti informaciją į apsaugos postą;

9.4. tarnybinės stotys ir kita įranga bei ją palaikančios sistemos turi būti Valstybiniame duomenų centre, kuris turi atitikti reikalavimus, numatytus Valstybinių duomenų centrų techninių reikalavimų apraše, patvirtintame Lietuvos Respublikos krašto apsaugos ministro 2019 m. lapkričio 18 d. įsakymu Nr. V-962 „Dėl Valstybinių duomenų centrų techninių reikalavimų aprašo patvirtinimo“.

10. Kitos priemonės, naudojamos elektroninės informacijos saugai užtikrinti:

10.1. kompiuterinės įrangos ir Įstaigos IS veikimas, Įstaigos IS administratorių, Įstaigos IS naudotojų ir Įstaigos IS vartotojų veiksmai ir kiti saugai svarbūs įvykiai fiksuojami ir registruojami žurnaliniuose įrašuose, kuriuose turi būti fiksuojama Įstaigos Duomenų saugos nuostatuose nurodyta informacija;

10.2. žurnaliniai įrašai turi būti kaupiami ir saugomi centralizuotai techninėje ar programinėje įrangoje, skirtoje audito duomenims saugoti, ne trumpiau kaip 60 (šešiasdešimt) kalendorinių dienų, ir analizuojami administratoriaus ne rečiau kaip kartą per mėnesį. Apie analizės rezultatus turi būti informuojamas Saugos įgaliotinis;

10.3. ne rečiau kaip kartą per metus atliekamas Įstaigos IS informacinių technologijų atitikties vertinimas ir Įstaigos IS rizikos vertinimas.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

11. Įstaigos IS elektroninę informaciją įvesti, keisti, atnaujinti ir naikinti gali tik autorizuoti Įstaigos IS naudotojai, kuriems Įstaigos naudotojų administravimo taisyklėse nustatyta tvarka yra suteiktos prieigos teisės prie Įstaigos IS ar jose tvarkomos informacijos ir duomenų.

12. Įstaigos IS taikomos įvestos elektroninės informacijos tikslumo, užbaigtumo ir patikimumo priemonės.

13. Siekiant nustatyti neteisėtus veiksmus su Įstaigos IS elektronine informacija bei šios informacijos vientisumo pažeidimus naudotojų veiksmai, jų darbo su Įstaigos IS laikas turi būti automatiškai registruojami žurnaliniuose įrašuose, apsaugotuose nuo neteisėto jame esančių duomenų panaudojimo, pakeitimo, iškraipymo ar sunaikinimo, kurie prieinami tik atitinkamas teises turintiems administratoriams – yra fiksuojamas paskutinį elektroninės informacijos pakeitimą atlikusį Įstaigos IS naudotojas ir pakeitimo laikas.

14. Įstaigos IS elektroninė informacija kitoms sistemoms teikiama ir (ar) gaunama iš jų vadovaujantis su šių sistemų valdytojais sudarytomis duomenų teikimo sutartimis. Duomenys kitoms informacinėms sistemoms teikiami XML formatu, teikiami ir iš jų gaunami šifruotu SSL kanalu, prieiga prie duomenų ribojama pagal IP adresą arba kitais duomenų teikimo sutartyse numatytais būdais, apimtimi, reguliarumu ir (ar) terminais;

15. IS elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo ar perdavimo (toliau – neleidžiama veikla) nustatymo tvarka:

15.1. IS administratoriai, užtikrindami elektroninės informacijos saugą, privalo naudoti visas įmanomas aparatines, programines ir administracines priemones skirtas apsisaugojimui nuo neleidžiamos veiklos;

15.2. siekiant patikrinti ar su Įstaigos IS tvarkoma elektronine informacija nėra vykdoma neleidžiama veikla, Įstaigos IS administratoriai kiekvieną darbo dieną privalo peržiūrėti Įstaigos IS programinės įrangos žurnalinius įrašus;

15.3. Įstaigos IS naudotojai, administratoriai ar aptarnaujantys darbuotojai, įtarę, kad su elektronine informacija buvo atlikti neteisėti veiksmai, privalo pranešti apie tai administratoriams ir (arba) Saugos įgaliotiniui;

15.4. Įstaigos IS administratorius, gavęs pranešimą apie galimą neteisėtą veiklą, turi nedelsiant reaguoti į Įstaigos IS naudotojų ar aptarnaujančio personalo pranešimus – imtis visų įmanomų veiksmų, reikalingų neteisėtai veiklai su užkirsti ir nedelsiant informuoti apie tai Saugos įgaliotinį (jei jo neinformavo Įstaigos IS naudotojas ar aptarnaujantys darbuotojai);

15.5. Saugos įgaliotinis, gavęs pranešimą apie neleidžiamą veiklą, turi įvertinti gautą informaciją ir priimti sprendimą dėl elektroninės informacijos saugos incidento tyrimo inicijavimo.

16. Įstaigos IS funkcionavimą užtikrinančios programinės ir techninės įrangos diegimą, priežiūrą, atnaujinimą, keitimą pagal gamintojų rekomendacijas atlieka Įstaigos IS administratoriai, kuriems priskirtos atitinkamos Įstaigos IS administravimo funkcijos arba aptarnaujantys darbuotojai.

17. Įstaigos programinės ir techninės įrangos keitimo ir atnaujinimo tvarka:

17.1. Įstaigos IS tarnybinėse stotyse programinę įrangą, reikalingą Įstaigos IS darbui, diegia ir tvarko Įstaigos IS administratorius arba aptarnaujantys darbuotojai;

17.2. organizuojami Įstaigos IS naudotojų darbo su nauja programine ir technine įranga mokymai;

17.3. naudojama tik sertifikuota programinė ir techninė įranga;

17.4. techninės, programinės ir sisteminės įrangos naujinimui galioja Įstaigos IS pokyčių įgyvendinimo taisyklės.

18. Atliekamas nuolatinis elektroninės informacijos atsarginis kopijavimas vadovaujantis šiomis nuostatomis:

18.1. atsarginės elektroninės informacijos kopijos daromos kiekvieną dieną į diskų masyvą ir į kopijavimo juostą, skirtą elektroninėms kopijoms saugoti;

18.2. elektroninės informacijos kopijų darymo faktas automatiškai fiksuojamas elektroniniame žurnale;

18.3. atsarginės elektroninės informacijos kopijos saugomos kitose nei tarnybinės stotys patalpose, kuriose užtikrinama tinkama apsauga;

18.4. informacija atsarginėse elektroninės informacijos kopijose turi būti šifruota, šifravimo raktai saugomi atskirai nuo kopijų. Prieiga prie atsarginių kopijų suteikiama tik įgaliotiems Įstaigos administratoriams;

18.5. ne rečiau kaip kartą per 6 (šešis) mėnesius Įstaigos IS administratoriaus arba aptarnaujantys darbuotojai turi atlikti elektroninės informacijos atkūrimo iš atsarginių kopijų bandymus, kurių metu turi būti atliekamas atsarginėse elektroninės informacijos kopijose esančių duomenų atstatymas. Atkūrimo iš atsarginių elektroninės informacijos kopijų bandymai yra protokoluojami.

19. Visa svarbi elektroninė informacija turi būti saugoma tarnybinių stočių įrangoje. Už asmeniniame kompiuteryje ar mobiliuose įrenginiuose esančios elektroninės informacijos atsarginių kopijų darymą yra atsakingas pats naudotojas.

20. Mobiliuosiuose įrenginiuose (nešiojamuosiuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir pan.), jeigu jie naudojami ne Įstaigos vidiniame kompiuterių tinkle, esanti Įstaigai svarbi informacija ir prisijungimo prie Įstaigos IS tvarkomos informacijos ir duomenų šifruojama, privaloma naudoti papildomas saugos priemones, kuriomis patvirtinama naudotojo tapatybė (slaptažodis, PIN kodas ir pan.).

21. Perduodant techninę įrangą išoriniams rangovams remontuoti turi būti užtikrinama, kad perduodamoje įrangoje nėra Įstaigos konfidencialios informacijos (išimami vidiniai diskai arba ištrinant informaciją naudojant specializuotą programinę įrangą, kad nebūtų galimybės jos atkurti.

22. Įstaigos IS pokyčiai (programinės ir techninės įrangos keitimas ir atnaujinimas) įgyvendinami laikantis nustatytų taisyklių:

22.1. visi Įstaigos IS pokyčiai (planavimas, projektavimas, kūrimas, testavimas, diegimas) atliekami Įstaigos IS valdytojo atstovo iniciatyva – pageidavimus dėl Įstaigos IS pokyčių gali registruoti Įstaigos darbuotojai Užimtumo tarnybos Informacinių technologijų problemų registravimo sistemoje (toliau – PRS). Registruotų pageidaujamų pokyčių reikalingumą pagal kompetenciją tvirtina Užimtumo tarnybos skyrių vedėjai ar jų pavaduotojai. Įstaigos IS pakeitimą užsakyti gali Įstaigos skyrių vedėjai ir jų pavaduotojai, siunčiant pakeitimo aprašymą Užimtumo tarnybos Infrastruktūros ir sistemų priežiūros skyriaus vedėjui ar jo pavaduotojui arba registruoti PRS;

22.2. Pokyčiai turi būti valdomi ir planuojami, apimant pokyčių identifikavimą, priskyrimą kategorijai (administracinis, organizacinis, techninis), įtakos vertinimą ir prioritetų nustatymą Įstaigos IS pokyčiai gali turėti skirtingą svarbą ir skirtingą pageidaujamą įgyvendinimo greitį:

22.2.1. skubūs darbai – pokyčiai, kuriuos reikia įgyvendinti nedelsiant įvykus Įstaigos IS ar jos posistemių ar kitų resursų sutrikimams ar klaidoms. Tai aukščiausio prioriteto darbai atliekami pirmiausiai, Įstaigos IS pokyčių užsakyme nurodomas būtinas pokyčių atlikimo terminas;

22.2.2. vidutinio skubumo darbai – kai vykdomas periodinis arba žinomas, ne kartą jau vykdytas Įstaigos IS pakeitimas, darbai, atliekami eilės tvarka, kai nėra skubių darbų,

Įstaigos IS pokyčio užsakyme nurodomas pageidaujamas pokyčių atlikimo terminas yra orientacinis pokyčių įdiegimo laikas;

22.2.3. neskubūs darbai – darbai, kuriuos reikia atlikti, bet jie nėra esminiai ir jų realizacija gali būti atidėta ilgesniam laikui, tokiems pakeitimams neturėtų būti nurodomas pakeitimų atlikimo pageidaujamas terminas;

22.3. turi būti nustatoma ir įvertinama su numatomais įgyvendinti pokyčiais susijusi rizika bei priemonės jai sumažinti;

22.4. pokyčių projektavimą ir kūrimą atlieka Įstaigos IS administratorius tam skirtoje kūrimo aplinkoje. Atliekant pakeitimo projektavimą ir kūrimą gali būti pasitelktos trečiosios šalys;

22.5. pagal pokyčių įtakos Įstaigos veiklai lygį, pakeitimai skirstomi į:

22.5.1. neturintys įtakos veiklai – smulkūs pakeitimai, kurie neturi įtakos esminiam veiklos funkcionalumui;

22.5.2. turintys įtakos atskiroms veiklos grupėms – tai pakeitimai, kurie vykdomi dalyje funkcionalumo ir gali turėti poveikį kai kurioms Įstaigos veikloms ar elektroninėms paslaugoms;

22.5.3. turintys įtakos visai veiklai – tai esminiai pokyčiai, kurie gali turėti įtakos visai veiklai ir yra rizika, kad turės įtakos klientų aptarnavimo kokybei;

22.6. prieš atliekant pokyčius, kurių metu gali iškilti grėsmė Įstaigos IS elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, visi pokyčiai turi būti išbandomi testavimo aplinkoje;

22.7. visi pokyčiai, galintys sutrikdyti ar sustabdyti Įstaigos IS veikimą, turi būti suderinti su Įstaigos IS duomenų valdymo įgaliotiniu ir apie galimus Įstaigos IS veikimo sutrikimus privalo ne vėliau kaip prieš 3 (tris) darbo dienas iki planuojamų pokyčių vykdymo pradžios raštu informuoti Infrastruktūros ir sistemų priežiūros skyriaus vedėją ir Saugos įgaliotinį;

22.8. diegiant pakeitimus, kurių metu galimi Įstaigos IS veikimo sutrikimai, Įstaigos IS administratorius arba Infrastruktūros ir sistemų priežiūros skyriaus vedėjo įgaliotas darbuotojas ne vėliau kaip 2 dienos iki planuojamų pokyčių vykdymo pradžios elektroniniu paštu informuoja naudotojus apie pokyčių darbų pradžią, pabaigą ir galimus Įstaigos IS veikimo sutrikimus;

22.9. visi pokyčiai gali būti diegiami tik suderinus diegimo laiką su Infrastruktūros ir sistemų priežiūros skyriaus vedėju arba pavaduotoju;

22.10. į gamybinę aplinką pokyčiai gali būti perkelti tik sėkmingai atlikus pokyčių testavimus, kurie turi būti protokoluojami. Pokyčiai, turintys įtakos atskiroms veiklos grupėms ar turintys įtaką visai veiklai gali būti diegiami tik prieš tai padarius duomenų bazių atsargines kopijas;

22.11. visi pokyčiai turi būti registruojami naudojant Įstaigos dokumentų valdymo sistemą ir apie tai informuojami Įstaigos IS administratoriai ir Įstaigos IS naudotojai. Naudotojams turi būti pateikiama visa reikalinga informacija apie Įstaigos IS pakeitimus, susijusius su planuojamais ar įvykdytais pokyčiais, esant poreikiui naudotojams ir susijusiems administratoriams turi būti rengiami mokymai.

IV SKYRIUS
REIKALAVIMAI, KELIAMI ĮSTAIGOS IS FUNKCIONAVIMUI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS

23. Paslaugų teikėjų prieigos prie Įstaigos IS lygiai ir sąlygos:

23.1. prieiga prie Įstaigos IS paslaugų teikėjams ir jų atstovams suteikiama tik tokio lygio, kuri yra būtina norint vykdyti sutartyje numatytus įsipareigojimus. Prieiga prie Įstaigos IS paslaugų teikėjams ir (arba) jų atstovams (aptarnaujantiems darbuotojams) suteikiama Įstaigos informacinių sistemų naudotojų administravimo taisyklėse nustatyta tvarka;

23.2. paslaugų teikėjo prieigos prie Įstaigos programinių ir techninių išteklių bei saugos reikalavimų laikymosi sąlygos turi būti apibrėžtos paslaugų teikimo sutartyse, kurių reikalavimų įgyvendinimo priežiūrą vykdo už sutartis vykdymą paskirti atsakingi asmenys;

23.3. sutartyse su Įstaigos IS funkcionalumui užtikrinti reikalingų paslaugų teikėjais turi būti numatyti informacijos konfidencialumo ir elektroninės informacijos saugos užtikrinimo reikalavimai bei numatyta atsakomybė už jų nesilaikymą;

23.4. paslaugų teikėjai, kuriems paslaugų teikimui yra būtina prieiga prie Įstaigos IS, privalo pasirašyti konfidencialumo įsipareigojimą, kuris galioja ir nutraukus sutartį ar pasibaigus jos galiojimui. Įstaigos IS administratorius, prieš suteikdamas prieigą prie asmens duomenų, kitokios konfidencialios informacijos arba ją apdorojančios Įstaigos IS, turi įsitikinti, kad aptarnaujantys darbuotojai yra pasirašę konfidencialumo pasižadėjimus ir privalo supažindinti aptarnaujančius darbuotojus su suteiktos prieigos prie duomenų saugyklų saugos reikalavimais ir sąlygomis;

23.5. administratorius suteikia aptarnaujantiems darbuotojams tik tokias prieigos prie Įstaigos IS teises, fizinę prieigą prie Įstaigos IS techninės ir programinės įrangos ir kitų resursų, kuri yra būtina norint atlikti arba vykdyti paslaugų teikėjo funkcijas paslaugų teikimo sutartyje nustatytomis sąlygomis ir tvarka;

23.6. Įstaigos IS administratorius atsako už programinių, techninių ir kitų prieigos prie Įstaigos IS išteklių organizavimą, suteikimą ir panaikinimą paslaugų teikėjui. Pasibaigus paslaugų teikimo sutarties galiojimui ar šią sutartį nutraukus, administratorius nedelsdamas, bet ne vėliau

kaip paskutinę sutarties galiojimo darbo dieną, panaikina visas aptarnaujančių darbuotojų prieigos prie Įstaigos IS teises.

24. Reikalavimai Įstaigos IS tarnybinių stočių patalpų, Įstaigos IS programinės įrangos, IS priežiūrai ir kitoms paslaugoms:

24.1. reikalavimai paslaugų teikėjams ir jų teikiamoms Įstaigos IS priežiūros paslaugoms nustatomi šių paslaugų teikimo sutartyse;

24.2. paslaugų teikėjas, darbų atlikėjas ar įrangos tiekėjas paslaugas, darbus ar įrangą, susijusią Įstaigos IS, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, privalo užtikrinti atitiktį Organizaciniams ir techniniams kibernetinio saugumo reikalavimams (tai turi būti iš anksto nustatyta pirkimo dokumentuose);

24.3. paslaugų teikėjas turi būti Įstaigai siūlomų programinių ir techninių produktų gamintojas arba šių produktų gamintojo oficialus atstovas ir turi užtikrinti kokybišką siūlomos programinės ir techninės įrangos garantinio aptarnavimo ir priežiūros paslaugų teikimą.

25. Įstaigos IS veiklą palaikančių sistemų (elektros energijos, šildymo, vėdinimo ir oro kondicionavimo bei kitos sistemos) kokybė atsižvelgiant į šių sistemų veiklai keliamus reikalavimus turi būti reguliariai tikrinama, siekiant užtikrinti tinkamą šių paslaugų teikimą ir sumažinti galimas šių paslaugų teikimo sutrikimo ir avarijos pasekmes.

V SKYRIUS
BAGIAMOSIOS NUOSTATOS

26. IS administratoriai, aptarnaujantis personalas ir Įstaigos IS naudotojai, pažeidę elektroninės informacijos saugą reglamentuojančių dokumentų ir kitų saugų Įstaigos IS elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

27. Taisyklės turi būti peržiūrimos ne rečiau kaip kartą per metus ir, nustačius poreikį, atnaujinamos. Papildomai taisyklės turi būti peržiūrimos atlikus rizikos ar saugos atitikties įvertinimą arba įvykus esminiams organizaciniams, sisteminiams ar kitokiems pokyčiams Įstaigoje. Už Taisyklių peržiūrą atsakingas Saugos įgaliotinis.

_____

Užimtumo tarnybos prie Lietuvos Respublikos
socialinės apsaugos ir darbo ministerijos
saugaus elektroninės informacijos tvarkymo
taisyklių
priedas

UŽIMTUMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS INFORMACINĖSE SISTEMOSE TVARKOMOS ELEKTRONINĖS INFORMACIJOS (JŲ GRUPIŲ) SĄRAŠAS

Eil. Nr.	Informacinė sistema	Tvarkomos elektroninės informacijos (jų grupių) sąrašas
1.	Lietuvos darbo biržos informacinė sistema (LDB IS, eDBirža)	Lietuvos darbo biržos informacinės sistemos nuostatų, patvirtintų Lietuvos darbo biržos prie Socialinės apsaugos ir darbo ministerijos direktoriaus 2010 m. rugpjūčio 5 d. įsakymu Nr. V-400 „Dėl Lietuvos darbo biržos informacinės sistemos nuostatų pakeitimo“ (Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus 2019 m. gruodžio 20 d. įsakymo Nr. V-462 redakcija) 17, 18 ir 19 punktuose nurodyta informacija.
2.	***Neteko galios nuo 2023-12-22***	
3.	Personalo valdymo informacinė sistema (PVS, Bonus)	Personalo valdymo informacinės sistemos nuostatų, patvirtintų Lietuvos darbo birža prie Socialinės apsaugos ir darbo ministerijos direktoriaus 2015 m. rugsėjo 7 d. įsakymu Nr. V-509 „Dėl Personalo valdymo informacinės sistemos nuostatų tvirtinimo“ 17 ir 18 punktuose nurodyta informacija.
4.	DocLogix (DVS)	Dokumentų valdymo sistemos aprašo, patvirtinto Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus 2022 m. rugsėjo 12 d. įsakymu Nr. V-279 „Dėl dokumentų valdymo sistemos aprašo patvirtinimo“ 8 punkte nurodyta informacija.
5.	Interneto svetainės	Interneto svetainių turinio valdymo sistemose (toliau – TVS): • TVS naudotojo vardas, pavardė, el. pašto adresas; • TVS naudotojui suteiktos teisės; • TVS naudotojų veiksmų apskaitos informacija;
5.1.	www.uzt.lt	• Užimtumo tarnybos veiklos naujienos; pranešimai spaudai; renginių, svarbiausių įvykių suvestinės; • Užimtumo tarnybos: – struktūra ir kontaktinė informacija; – teisinė informacija: teisės aktai; teisės aktų projektai; tyrimai ir analizės; teisės aktų pažeidimai; galiojančio teisinio reguliavimo poveikio *ex post* vertinimas; – veiklos sritys; – pranešėjų apsauga; – korupcijos prevencija;

		– administracinė informacija: nuostatai; planavimo dokumentai; darbo užmokestis; paskatinimai ir apdovanojimai; viešieji pirkimai; biudžeto vykdymo ataskaitų rinkiniai; finansinių ataskaitų rinkiniai; ūkio subjektų priežiūra; tarnybiniai lengvieji automobiliai; lėšos veiklai viešinti; – paslaugos; – atviri duomenys; – asmens duomenų apsauga; – nuorodos; – dažniausiai užduodami klausimai; – konsultavimasis su visuomene; – naujienlaiškių prenumeratos apskaitos informacija: el. pašto adresai.
5.2.	https://eures.uzt.lt/	• EURES Lietuva: – informacija apie EURES; – naujienos ir renginiai; – darbo pasiūlymai; – darbo ieškantiems asmenims; – darbdaviams; – migrantams; – gyvenimo ir darbo sąlygos ES, EEE šalyse; – nedarbo socialinio draudimo išmokos eksportas; – EURES Targeted Mobility Scheme (TMS) darbo mobilumo programa; – Nuorodos; – naujienlaiškių prenumeratos apskaitos informacija: el. pašto adresai.
5.3.	https://soczemelapis.uzt.lt/	• Socialinės pagalbos žemėlapis – registruotų juridinių asmenų pavadinimai, veiklos vykdymo vieta, kontaktinė informacija, teikiamų paslaugų klasifikatorius; • Nuorodos.
5.4.	https://galilietuva.lt/	• Projekto „Gal į Lietuvą“: – veiklos naujienos; pranešimai spaudai; renginių, svarbiausių įvykių suvestinės; – Pakviesk (el. laiškų siuntimo įrankis): gavėjo el. paštas, vardas, šalis, siuntėjo vardas ir pavardė; – Gera dirbti – informaciniai pranešimai; – Darbo pasiūlymai - darbo pasiūlymų paieškos įrankis; – Verslas – informaciniai pranešimai; – naujienlaiškių prenumeratos apskaitos informacija: el. pašto adresai.

PATVIRTINTA
Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus 2021 m. kovo 19 d. įsakymu Nr. V-113
(Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus 2022 m. rugsėjo 27 d. įsakymo Nr. V-298 redakcija)

UŽIMTUMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų naudotojų administravimo taisyklės (toliau – Naudotojų administravimo taisyklės) reglamentuoja Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos (toliau – Užimtumo tarnyba, Įstaiga) valdomų informacinių sistemų (toliau – Įstaigos IS) naudotojų prieigos teisių suteikimą, pakeitimą ir panaikinimą, naudotojų įgaliojimus, teises, pareigas, jų administravimo ir supažindinimo su saugos dokumentais tvarką.

2. Naudotojų administravimo taisyklėse vartojamos sąvokos suprantamos taip, kaip jos 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“, Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. gruodžio 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizaciniai ir techniniai kibernetinio saugumo reikalavimai), Lietuvos Respublikos standartuose LST ISO/IEC 27002:2014 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“ ir LST ISO/IEC 27001:2013 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“, Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo

ministerijos informacinių sistemų duomenų saugos nuostatuose ir kituose saugų duomenų tvarkymą reglamentuojančiuose teisės aktuose.

3. IS naudotojų administravimo taisyklės taikomos visiems Užimtumo tarnybos valdomų informacinių sistemų naudotojams, administratoriams, Saugos įgaliotiniui.

4. IS naudotojams prieiga prie elektroninės informacijos suteikiama vadovaujantis šiais principais:

4.1. naudotojams prieigos prie Įstaigos IS teisės suteikiamos vadovaujantis principais „būtina darbui“ ir „būtina žinoti“, t. y. Įstaigos IS naudotojui turi būti suteikiamos pagal jo užimamas pareigas minimalios ir tik jo tiesioginėms funkcijoms vykdyti reikalingos prieigos prie Įstaigos IS teisės;

4.2. konfidencialumo užtikrinimas – prieigą prie Įstaigos IS išteklių ir tvarkomos elektroninės informacijos gali gauti tik tie Įstaigos IS naudotojai, kuriems tokia teisė yra suteikta;

4.3. vientisumo užtikrinimas – Įstaigos IS saugomus duomenis tvarkyti (peržiūrėti, įrašyti, koreguoti, ištrinti ir su duomenimis atlikti kitus veiksmus) gali tik tokias teises turintis Įstaigos IS naudotojas;

4.4. pasiekiamumo užtikrinimas – Įstaigos IS ištekliai ir tvarkoma elektroninė informacija prieigos teises turintiems naudotojams pasiekiama jiems reikiamu metu;

4.5. apskaita (veiksmų nepaneigiamumu) – atitinkamus veiksmus atlikę Įstaigos IS naudotojai negali turėti galimybės paneigti veiksmų Įstaigos IS atlikimo, t. y. Įstaigos IS naudotojų atlikti veiksmai apskaitomi (registruojami), taip užtikrinant jų atsakomybę už atliktus veiksmus;

4.6. prieiga prie Įstaigos IS saugomos elektroninės informacijos ir teisė ją keisti suteikiama tik Įstaigos IS naudotojui patvirtinus savo tapatybę, t. y. įvedus Įstaigos IS naudotojo vardą ir slaptažodį arba dviejų veiksnių tapatumo patvirtinimo priemonėmis;

4.7. Įstaigos IS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą Įstaigos IS administratoriaus paskyrą, kuria naudojantis negalima atlikti Įstaigos IS naudotojo funkcijų;

4.8. Įstaigos IS naudotojams negali būti suteikiamos Įstaigos IS administratoriaus teisės.

II SKYRIUS
ĮSTAIGOS IS NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

5. Įstaigos IS naudotojai gali naudotis tik tomis informacinėmis sistemomis, jų dalimi ar jos komponentais, ir juose tvarkoma elektronine informacija, prie kurių prieigą jiems suteikė

Įstaigos IS administratorius pagal naudotojo kompetenciją. Naudodamiesi Įstaigos IS ar joje tvarkoma informacija naudotojai turi:

5.1. susipažinti su Įstaigos Saugos dokumentais ir kitais teisės aktais, reglamentuojančiais elektroninės informacijos saugą ir (arba) kibernetinį saugumą (toliau – Saugos dokumentai), Įstaigos IS naudojimo instrukcijomis (naudotojų vadovais, procedūromis) ir jų laikytis;

5.2. naudoti Įstaigos kompiuterinę ir programinę įrangą (toliau – Įranga) vadovaujantis Įstaigos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklėmis, suteiktą Įrangą, programas ir informaciją naudoti tik darbo funkcijų atlikimui;

5.3. rinkti, tvarkyti, perduoti, saugoti, naikinti ar kitaip naudoti Įstaigos IS saugomą elektroninę informaciją tik atlikdami savo tiesiogines funkcijas;

5.4. užtikrinti elektroninės informacijos konfidencialumą ir vientisumą, vadovaujantis Naudotojų administravimo taisyklėse ir kituose Saugos dokumentuose nustatytais reikalavimais;

5.5. laikytis „švaraus stalo ir ekrano“ politikos – kiekvieną kartą nors ir trumpam palikdami savo darbo vietą, užtikrinti, kad pašaliniai asmenys negalėtų susipažinti su informacija – atsijungti nuo IS, įjungti ekrano užsklandą;

5.6. baigus darbą, atsijungti nuo Įstaigos IS;

5.7. nedelsiant pranešti Saugos įgaliotiniui ar Įstaigos IS administratoriui apie pastebėtus IS naudojimo sutrikimus, neveikiančią ar netinkamai veikiančią sistemą ar jos saugos užtikrinimo priemones, grėsmes Įstaigos kompiuterių tinklui ar Įstaigos IS duomenų saugumui (kompiuterinių virusų patekimas į kompiuterį, nesankcionuotas patekimas į kompiuterių tinklą, nesankcionuoti Įstaigos darbuotojų ar trečiųjų šalių veiksmai su Įstaigos IS duomenims ir kt.) Užimtumo tarnybos Informacinių technologijų problemų registravimo sistemoje (toliau – PRS) arba el. paštu itpagalba@uzt.lt;

5.8. atliekant darbo funkcijas, susipažinus su asmens duomenimis, neatkleisti (neviešinti) asmens duomenų, jei asmens duomenys neskirti skelbti viešai. Ši pareiga galioja ir pasibaigus darbo santykiams Įstaigoje;

5.9. naudoti suteiktą Įrangą, programas tik darbo funkcijų atlikimui;

5.10. vykdyti Saugos įgaliotinio ir (arba) Įstaigos IS administratoriaus nurodymus dėl Įstaigos IS ir kompiuterinės įrangos naudojimo.

6. Naudotojams draudžiama:

6.1. savavališkai ar savarankiškai keisti jiems paskirtos Įrangos konfigūraciją, šalinti įrangos gedimus;

6.2. savavališkai naudoti ir organizuoti nenustatytus kompiuterių ryšius iš darbo vietos su internetu ar kitais išorės tinklais;

6.3. naudoti Įrangą, Įstaigos IS ir jos duomenų bazes, interneto ir elektroninio pašto teikiamas galimybes kitiems tikslams, nesusijusiems su darbinių funkcijų atlikimu;

6.4. paskirtoje Įrangoje naudoti ir platinti Įstaigos kompiuteriniuose tinkluose ar kitais būdais nelicencijuotą programinę įrangą;

6.5. platinti, atskleisti kitiems asmenims darbui su Įranga jiems suteiktus prieigos vardus, slaptažodžius, kodus, įrangos konfigūracijos ar kitus duomenis;

6.6. turėti ir naudoti programas, skaitančias, peržiūrinčias ir analizuojančias lokalius kompiuterių tinklus ir jais perduodamą informaciją;

6.7. keisti, atnaujinti, įdiegti ar šalinti programinę įrangą (ši nuostata netaikoma automatiniam programinės įrangos atnaujinimui);

6.8. leisti naudoti jam paskirtą Įrangą pašaliniams asmenims;

6.9. dirbant su Įranga ir šalia jos vartoti maistą, gėrimus ar naudoti kitas medžiagas bei priemones, galinčias pakenkti Įrangai;

6.10. išnešti Įrangą iš Įstaigos teritorijos prieš tai nesuderinus su savo tiesioginiu vadovu arba atsakingu už Įranga asmeniu, išskyrus tam tikslui skirtą mobiliąją kompiuterinę įrangą. Šis draudimas netaikomas kompiuterinės įrangos remonto ir priežiūros funkcijas atliekantiems Įstaigos darbuotojams, bei šias funkcijas atliekančių paslaugų teikėjų įgaliotiems asmenims, su kuriais sudarytos kompiuterinės įrangos remonto ir priežiūros sutartys.

7. Atleidus darbuotoją iš darbo, taip pat išleidžiant nėštumo ir gimdymo atostogų bei suteikiant vaiko priežiūros atostogas, paskutinę darbo dieną darbuotojas privalo:

7.1. grąžinti jam paskirtą Įrangą. Atsiskaitymo lape (Užimtumo tarnybos vidaus tvarkos taisyklių 3 priedas) pasirašo materialiai atsakingas Įstaigos darbuotojas;

7.2. perduoti jo funkcijas perimančiam darbuotojui ar tiesioginiam vadovui sukurtas elektronines bylas ir kitą elektroninę informaciją;

7.3. ištrinti iš kompiuterio ir informacijos pasikeitimui skirtų katalogų elektroninę informaciją, kuri jo tiesioginio vadovo sprendimu neturi būti išsaugoma.

8. IS administratoriai, atsakingi už informacinės sistemos infrastuktūrą, turi teisę fiziškai prieiti prie techninės ir sisteminės programinės įrangos ir vykdyti IS techninės priežiūros funkcijas, kad būtų užtikrintas nepertraukiamas Įstaigos IS techninės ir programinės įrangos veikimas. Įstaigos IS administratoriai atsako už:

8.1. Įstaigos IS funkcionavimą užtikrinančios techninės ir programinės įrangos, duomenų bazių, kompiuterinių tinklų infrastruktūros bei informacinių technologijų paslaugų administravimą bei priežiūrą;

8.2. Įstaigos IS naudotojų registravimą ir registravimo vardų skyrimą tarnybinėse stotyse, prieigos prie Įstaigos IS teisių nustatymą;

8.3. Įstaigos IS komponentų sąrankos ir Įstaigos IS būsenos rodiklių patikrinimą, Įstaigos IS sąrankos aprašymo dokumentų parengimą;

8.4. atsarginių Įstaigos IS elektroninės informacijos kopijų darymą bei informacijos atkūrimo iš atsarginių kopijų išbandymą;

8.5. Įstaigos IS pažeidžiamų vietų nustatymą, Įstaigos IS saugos priemonių parinkimą ir įdiegimą bei jų atitiktį Saugos dokumentų reikalavimams.

9. Įstaigos IS administratoriai turi teisę:

9.1. registruoti IS naudotojus centralizuotoje kompiuterių tinklo naudotojų prieigos sistemoje (*Active Directory*) (toliau – AD), administruoti naudotojų paskyras, kurti naudotojų grupes AD, suteikti bei administruoti IS naudotojų prieigos teises, jas redaguoti, keisti ir panaikinti;

9.2. pateikti užklausas dėl Įstaigos IS naudotojų duomenų patikslinimo;

9.3. matyti Įstaigos IS naudotojų identifikavimo ir suteiktų teisių duomenis ir atliktus veiksmus;

9.4. diegti Įstaigos IS atnaujinimus ir pakeitimus bei užtikrinti tinkamą duomenų bazių ir posistemių funkcionavimą;

9.5. skaityti, kurti, atnaujinti, naikinti Įstaigos IS informaciją, atlikti paiešką Įstaigos IS pagal pasirinktus paieškos kriterijus.

III SKYRIUS
SAUGAUS ELEKTRONINĖS INFORMACIJOS TEIKIMO INFORMACINĖS SISTEMOS NAUDOTOJAMS KONTROLĖS TVARKA

10. Įstaigos IS naudotojo registravimo tvarka:

10.1. Pirminė naudotojo registracija vykdoma užregistruojant naudotoją AD, nesuteikiant prieigos teisių prie Įstaigos IS tvarkomos elektroninės informacijos, tačiau sukuriant unikalų prisijungimo vardą ir pirminį prisijungimo slaptažodį bei perduodant jį naudotojui. Registruojant naują Įstaigos IS naudotoją, įvedama tokia informacija: vardas, pavardė, pareigos, darbo vietos duomenys (įstaigos pavadinimas, skyrius, poskyris) ir kontaktinė informacija (telefono numeris, elektroninio pašto adresas);

10.2. naudotojo prieigos teisės prie konkrečių Įstaigos IS ar jų modulių ir jose tvarkomos elektorinės informacijos suteikiamos pagal darbuotojo tiesioginio vadovo prašymą, kuris užregistruojamas PRS bei nurodant reikalingus Įstaigos IS modulius bei prieigos teises;

10.3. pirminę naudotojo registraciją, o vėliau prieigos teisių suteikimą, pakeitimą ir panaikinimą, naudojant teisių ir rolių valdymo priemones, atlieka IS administratoriai;

10.4. prieigos teisės prie konkrečių Įstaigos IS naudotojui suteikiamos atsižvelgiant į jo pareigas ir atliekamas darbo funkcijas – naudotojų teisių ir rolių valdymo priemonės suteikia kiekvienam Įstaigos IS naudotojui tik jo funkcijoms vykdyti reikalingas teises ir prieigą prie Įstaigos IS elektroninės informacijos bei Įstaigos IS funkcionalumo;

10.5. prieigos teisės Įstaigos IS naudotojui suteikiamos tik jam susipažinus su Saugos dokumentais, o teisė tvarkyti asmens duomenis Įstaigos IS naudotojui suteikiama tik jam pasirašius pasižadėjimą saugoti asmens duomenų paslaptį;

10.6. naudotojui negali būti suteiktos Įstaigos IS administratoriaus teisės;

10.7. draudžiama naudoti bendras prieigos teises – kiekvienas naudotojas turi būti unikaliai identifikuojamas.

11. Įstaigos IS naudotojui teisė dirbti su konkrečia Įstaigos IS informacija sustabdoma ir prieigos teisės blokuojamos, kai naudotojas nesinaudoja Įstaigos IS ilgiau kaip 3 mėnesius. Įstaigos IS administratoriaus teisės dirbti su konkrečia Įstaigos IS turi būti sustabdoma ir prieigos teisės blokuojamos, jei Įstaigos IS administratorius nesinaudoja Įstaigos IS ilgiau kaip 2 mėnesius. Kai tai leidžia naudojamos technologijos, turi būti taikomas automatinis Įstaigos IS naudotojų prieigos teisių blokavimas.

12. Įstaigos IS naudotojui ar Įstaigos IS administratoriui prieigos teisės prie Įstaigos IS turi būti panaikintos nedelsiant jei Įstaigos IS naudotojas ar Įstaigos IS administratorius:

12.1. yra nušalinamas nuo darbo (pareigų);

12.2. neatitinka nustatytų Įstaigos IS naudotojo ar Įstaigos IS administratoriaus kvalifikacinių reikalavimų;

12.3. praranda patikimumą;

12.4. pasibaigia darbo santykiai Įstaigoje.

13. Nutraukiant darbo santykius su Įstaigos IS naudotoju, atsakingas Žmogiškųjų išteklių valdymo skyriaus specialistas užregistruoja pranešimą apie darbo santykių nutraukimą PRS ne vėliau kaip paskutinę darbuotojo darbo Įstaigoje dieną.

14. Įstaigos IS naudotojo ar Įstaigos IS administratoriaus, su kuriuo nutraukiami darbo santykiai, prieiga prie Įstaigos IS panaikinama nedelsiant, bet ne vėliau kaip paskutinės naudotojo darbo dienos 15 valandą, o prieiga prie kompiuterių tinklo išteklių – ne vėliau kaip po mėnesio. Įstaigos IS naudotojo ar Įstaigos IS administratoriaus prieigos teises, įskaitant ir prieigą prie jo elektroninės pašto dėžutės, panaikina IS administratorius, atsakingas už naudotojų prieigos teisių administravimą.

15. Įstaigos IS naudotojo tapatybės nustatymo tvarka:

15.1. Įstaigos IS naudotojų tapatybė nustatoma pagal suteiktą unikalų prisijungimo prie Įstaigos IS identifikatorių (naudotojo vardą) ir slaptažodį, užregistruotą AD, kurį suteikia Įstaigos IS administratorius arba taikant dviejų veiksnių tapatumo patvirtinimo priemones;

15.2. draudžiama naudoti jau esantį arba anksčiau naudotą Įstaigos IS naudotojo vardą registruojant kitą Įstaigos IS naudotoją;

15.3. Įstaigos IS naudotojo vardas ir slaptažodis negali būti atskleidžiami kitiems asmenims;

15.4. draudžiama naudotis kito Įstaigos IS naudotojo prieigos teisėmis;

15.5. Įstaigos IS naudotojo vardas panaikinamas, pasibaigus darbuotojo darbo santykiams.

16. Įstaigos IS naudotojui neatliekant jokių veiksmų Įstaigos IS turi užsirakinti, kad toliau naudotis Įstaigos IS būtų galima tik pakartotinai patvirtinus savo tapatybę. Ilgiausias neaktyvumo laikas, kuriam pasibaigus Įstaigos IS naudotojo ryšio sesijos yra automatiškai nutraukiamos, yra 15 minučių.

17. Įstaigos IS naudotojui neteisingai įvedus slaptažodį 5 kartus iš eilės, naudotojo paskyra užrakinama ir Įstaigos IS naudotojui neleidžiama patvirtinti savo tapatybės 15 minučių.

18. Įstaigos IS naudotojo slaptažodžio naudojimo tvarka:

18.1. slaptažodžiai negali būti saugomi ar perduodami atviru tekstu ar užšifruojami nepatikimais algoritmais;

18.2. pirminis ar laikinas prisijungimo slaptažodis, Saugos įgaliotinio sprendimu, Įstaigos IS naudotojams gali būti perduodamas atviru tekstu, tačiau atskirai nuo prisijungimo vardo jei Įstaigos IS naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių Įstaigos IS naudotojui perduoti slaptažodį šifruotu kanalu ar saugiu elektroninių ryšių tinklu;

18.3. gavęs prieigos teises prie Įstaigos kompiuterinio tinklo, naudotojo vardą ir slaptažodį, naudotojas turi saugoti jam suteiktus prisijungimo duomenis ir neperduoti jų kitiems naudotojams ar kitiems asmenims;

18.4. pirmojo prisijungimo prie kompiuterių tinklo jam suteiktu prisijungimo vardu ir slaptažodžiu, programinė įranga pareikalauja pasikeisti administratoriaus suteiktą pirminį prisijungimo slaptažodį, vėliau slaptažodis turi būti keičiamas reguliariai ne rečiau kaip kas 60 (šešiasdešimt) kalendorinių dienų;

18.5. draudžiama atskleisti slaptažodį perduodant jį elektroniniu būdu, telefonu, užrašytą ant popieriaus slaptažodį paliekant matomoje vietoje ar kitais būdais sudarant galimybę slaptažodį sužinoti pašaliniams asmenims.

19. Reikalavimai Įstaigos IS naudotojų slaptažodžiams:

19.1. slaptažodis turi būti sudarytas iš didžiųjų raidžių, mažųjų raidžių, skaitmenų ir specialiųjų simbolių;

19.2. slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

19.3. draudžiama slaptažodyje naudoti reikšminius žodžius arba asmeninio pobūdžio informaciją;

19.4. Įstaigos IS naudotojo slaptažodis turi būti keičiamas nedelsiant, bet ne vėliau kaip iki darbo dienos pabaigos jei kilo įtarimas, kad slaptažodį sužinojo ar galėjo sužinoti pašaliniai asmenys;

19.5. keičiant slaptažodį programinė įranga neleidžia naudoti prieš tai buvusių 20 naudotų slaptažodžių;

19.6. pamiršęs slaptažodį, Įstaigos IS naudotojas turi kreiptis į Įstaigos IS administratorių su prašymu suteikti naują laikiną slaptažodį, kurį privalo pasikeisti pirmą kartą prisijungęs prie Įstaigos IS.

20. Papildomi reikalavimai Įstaigos IS administratorių slaptažodžiams:

20.1. slaptažodį turi sudaryti ne mažiau kaip iš 12 simbolių;

20.2. Įstaigos IS administratoriaus slaptažodis turi būti keičiamas ne rečiau kaip kartą per 30 (trisdešimt) kalendorinių dienų arba jei kilo įtarimas, kad slaptažodį sužinojo ar galėjo sužinoti pašaliniai asmenys.

21. Įstaigos IS administratorių tapatybei patvirtinti turi būti naudojama dviejų veiksnių tapatumo patvirtinimo priemonės jeigu Įstaigos IS palaiko tokį funkcionalumą.

22. Pasikeitus Įstaigos IS naudotojo pareigoms ar vykdomoms funkcijoms, jo prieigos teisės prie Įstaigos IS turi būti panaikinamos ir sukuriamos naujos, atitinkančios pasikeitusias darbuotojo pareigas.

23. Įstaigos IS naudotojų prieigos teisės prie elektroninės informacijos panaikinamos šiais atvejais:

23.1. įgaliojimus turinčiam asmeniui pateikus raštiško nurodymo kopiją Įstaigos IS valdytojui dėl Įstaigos IS naudotojo pakeitimo ar jo prieigos prie IS panaikinimo;

23.2. Įstaigos IS naudotojui netekus teisės naudotis elektronine informacija;

23.3. nustačius Įstaigos IS naudotojo neteisėtą naudojimąsi elektronine informacija;

23.4. įtarus Įstaigos IS naudotojo prisijungimo vardo ir/ar slaptažodžio prie Įstaigos IS atskleidimą.

24. Įstaigos IS naudotojui teisė dirbti su konkrečia elektronine informacija gali būti ribojama ar sustabdoma, kai:

24.1. Įstaigos IS naudotojas atostogauja;

24.2. vykdomas Įstaigos IS naudotojo tarnybinis ar drausmės tyrimas;

24.3. kitais atvejais, gavus Įstaigos ar jos struktūrinio padalinio, kuriame dirba Įstaigos IS naudotojas, vedėjo prašymą.

25. Nuotolinė prieiga prie Įstaigos IS gali būti suteikiama tik aptarnaujantiems darbuotojams ir mobiliųjų darbo vietų naudotojams Įstaigos ar teritorinių Klientų aptarnavimo departamentų direktorių ar jų pavaduotojų nurodymu. Nuotolinė prieiga galima tik naudojantis saugiu šifruotu kanalu (*SSL VPN* tuneliu).

26. Prisijungti prie Įstaigos IS nuotoliniu būdu galima tik iš Įstaigai nuosavybės teise priklausančios įrangos (kompiuterių ir kitų mobiliųjų įrenginių) išskyrus atvejus, kai prie Įstaigos IS jungiasi aptarnaujantys darbuotojai. Įstaigos IS, atliekančios nutolusio prisijungimo autentifikavimą, turi drausti automatiškai išsaugoti slaptažodžius.

27. Aptarnaujantys darbuotojai Įstaigos IS priežiūros funkcijas atlieka naudodami atskirą, tam skirtą administratoriaus identifikatorių, kuriuo naudojantis nebūtų galima atlikti Įstaigos IS naudotojo funkcijų.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

28. Naudotojų administravimo taisyklės peržiūrimos ir, jei reikia, turi būti keičiamos ne rečiau kaip kartą per metus, taip pat po to, kai atliekamas rizikos įvertinimas ar informacinių technologijų saugos atitikties vertinimas arba kai Įstaigoje įvyksta esminių organizacinių, sisteminių ar kitokių pokyčių.

29. Už Naudotojų administravimo taisyklių nesilaikymą IS naudotojai ir IS administratoriai atsako teisės aktų nustatyta tvarka.

_____

Priedo pakeitimai:
Nr. V-252, 2023-12-21, paskelbta TAR 2023-12-21, i. k. 2023-24884

Priedo pakeitimai:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

PATVIRTINTA
Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus 2021 m. kovo 19 d. įsakymu Nr. V-113
(Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus 2022 m. rugsėjo 27 d. įsakymo Nr. V-298 redakcija)

UŽIMTUMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų veiklos tęstinumo valdymo planas (toliau – Valdymo planas) reglamentuoja Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos (toliau – Užimtumo tarnyba, Įstaiga) valdomų informacinių sistemų (toliau – Įstaigos IS) ir jos teikiamų funkcijų tęstinumo užtikrinimą, įvykus elektroninės informacijos saugos ar kibernetiniam incidentui (toliau – Incidentas), dėl kurio susidarė ekstremali situacija, taip pat nustato Įstaigos IS valdytojo ir tvarkytojų veiksmus įvykus Incidentui, kurio metu gali kilti pavojus tvarkomos elektroninės informacijos konfidencialumui, vientisumui ir prieinamumui.

2. Valdymo planas parengtas vadovaujantis:

2.1. Lietuvos Respublikos kibernetinio saugumo įstatymu;

2.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

2.3. Bendrųjų elektroninės informacijos saugos reikalavimu 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 – Bendrųjų elektroninės informacijos saugos reikalavimu aprašas);

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

2.5. Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

2.6. Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų duomenų saugos nuostatais (toliau – Saugos nuostatai);

2.7. Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašu, patvirtintu 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 – Techninių saugos reikalavimų aprašas).

3. Valdymo plane vartojamos sąvokos:

3.1. **Duomenų centras** – specializuotos patalpos, skirtos centrinių ir tinklo kompiuterių įrangai talpinti, kuriose įrengtos minėtos įrangos nuolatiniam veikimui bei saugai užtikrinti būtinos inžinerinės sistemos (vėdinimo ir kondicionavimo, nuolatinio elektros maitinimo, priešgaisrinės saugos ir įėjimo kontrolės sistemos).

3.2. **Ekstremali situacija** – incidentas, kurio metu sutrinka arba neveikia bent viena Įstaigos IS (ar jos dalis), galinti turėti neigiamą įtaką pagrindiniams Užimtumo tarnybos veiklos procesams.

3.3. **Veiklos tęstinumo valdymo grupė** – Užimtumo tarnybos direktoriaus įsakymu sudaryta grupė koordinuojanti Įstaigos IS veiklos atkūrimą esant ekstremaliai situacijai bei užtikrinanti tęstinumui kylančių grėsmių valdymą ir sprendimų, reikalingų Įstaigos IS veiklos atkūrimui priėmimą.

3.4. **Veiklos atkūrimo grupė** – grupė užtikrinanti Įstaigos IS veiklos atkūrimą ir veikimą bei atskaitinga Valdymo grupei, esant ekstremaliai situacijai.

4. Kitos Valdymo plane naudojamos sąvokos suprantamos taip, kaip jos apibrėžtos Valdymo plano 2 punkte nurodytuose teisės aktuose ir kituose Įstaigos elektroninės informacijos saugą ir kibernetinį saugumą reglamentuojančiuose dokumentuose (toliau – Saugos dokumentai).

5. Valdymo planas įsigalioja įvykus Incidentui, jei nustatoma, kad standartinėmis incidentų valdymo priemonėmis Įstaigos IS įprastinės veiklos atkurti per maksimalų leistiną paslaugos neveikimo laiką, nustatytą Įstaigos Saugos nuostatų 1 priede, nepavyks. Apie tai Saugos įgaliotinis informuoja Užimtumo tarnybos direktorių ir Valdymo grupės vadovą, kuris priima sprendimą dėl Valdymo plano įsigaliojimo ir sušaukia Valdymo grupės posėdį.

6. Valdymo planas privalomas Įstaigos IS valdytojui, tvarkytojams, saugos įgaliotiniui, Įstaigos IS administratoriams ir Įstaigos IS naudotojams bei aptarnaujantiems darbuotojams.

7. Valdymo plano įgyvendinimo nuostatos:

7.1. Saugos įgaliotinis dalyvauja Valdymo grupėje ir teikia jai informaciją apie Incidentą, sukėlusį ekstremalią situaciją;

7.2. Įstaigos IS administratoriai užtikrina Įstaigos IS veiklos atkūrimą ir dalyvauja Atkūrimo grupės veikloje;

7.3. Įstaigos IS naudotojai privalo laikytis Valdymo plano reikalavimų bei vykdyti ir Valdymo bei Atkūrimo grupių reikalavimus.

8. Reaguojant į Incidentus ir juos valdant, vykdomi veiksmai, nurodyti informacinių sistemų veiklos atkūrimo detaliajame plane (toliau – Detalusis planas), ir vadovaujamasi šiais principais:

8.1. gyvybės ir sveikatos apsaugos – pirmiausia privalo būti užtikrinta Užimtumo tarnybos valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis (toliau – darbuotojai) gyvybė ir sveikata, kol trunka ekstremali situacija ir likviduojami Incidento padariniai;

8.2. turto apsaugos – privalo būti užtikrinta Įstaigos turto apsauga, kol trunka ekstremali situacija ir likviduojami Incidento padariniai;

8.3. Įstaigos IS veiklos laipsniško atkūrimo – pirmiausia atkuriamos būtinos Įstaigos veiklai užtikrinti IT infrastruktūros veikimas ir informacinės sistemos bei užtikrinamas jų prieinamumas pagal Valdymo plano 1 priede pateiktą eiliškumą.

9. Įstaigos IS yra laikoma atkurta jeigu:

9.1. yra atkurtas Incidento metu sutrikusių Įstaigos IS prieinamumas, užtikrintas informacijos konfidencialumas ir vientisumas;

9.2. IS elektroninė informacija yra teisinga ir nuolat atnaujinama;

9.3. IS nustatyta tvarka gauna elektroninę informaciją iš kitų susijusių informacinių sistemų ir registrų;

9.4. IS elektroninė informacija teikiama duomenų gavėjams duomenų teikimo sutartyse nustatytomis sąlygomis arba pagal duomenų gavėjo prašymą;

9.5. IS naudotojai gali atlikti savo funkcijas ir Įstaigos IS vartotojai gauti paslaugas, naudodamiesi Įstaigos IS.

10. Įstaigos IS ir IT infrastruktūros atkūrimo prioritetai nustatyti Valdymo plano 1 priede.

11. Finansinių ir kitų išteklių, reikalingų Įstaigos IS veiklai atkurti, įvykus ekstremaliai situacijai, šaltinius ir pobūdį numato Valdymo grupė kiekvienos ekstremalios situacijos atveju ir teikia Įstaigos direktoriui.

12. Elektroninės informacijos saugos incidentai, kiti incidentai, nesukėlę ekstremalios situacijos, valdomi Informacijos saugos incidentų valdymo procedūroje nustatyta tvarka.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

13. Veiklos tęstinumo valdymo grupės sudėtis (toliau – Valdymo grupė):

13.1. Užimtumo tarnybos direktorius (veiklos tęstinumo valdymo grupės vadovas);

13.2. Užimtumo tarnybos kancleris (veiklos tęstinumo valdymo grupės vadovo pavaduotojas);

13.3. Užimtumo tarnybos saugos įgaliotinis;

13.4. Infrastruktūros ir sistemų priežiūros skyriaus vedėjas;

13.5. Užimtumo tarnybos duomenų apsaugos pareigūnas;

13.6. Informacinių technologijų paslaugų teikėjo – Informacinės visuomenės plėtros komiteto, juridinio asmens kodas 188772433 (toliau – IT paslaugų teikėjas) atstovas (toliau – IT paslaugų teikėjo atstovas).

14. Valdymo grupė atlieka šias funkcijas:

14.1. analizuoja situaciją ir priima sprendimus Įstaigos IS veiklos tęstinumo valdymo klausimais;

14.2. skelbia ir atšaukia ekstremalią situaciją;

14.3. bendrauja su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

14.4. bendrauja su susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis;

14.5. informuoja Nacionalinį kibernetinio saugumo centrą apie Įstaigos IS įvykusius kibernetinius incidentus, nurodytus Nacionaliniame kibernetinių incidentų valdymo plane ir taikytas kibernetinių saugos incidentų valdymo priemones Kibernetinių incidentų valdymo ir Nacionalinio kibernetinio saugumo centro informavimo tvarkos apraše numatyta tvarka (2 priedas);

14.6. bendrauja su teisėsaugos ir kitomis institucijomis, Įstaigos darbuotojais ir kitomis interesų grupėmis;

14.7. kontroliuoja finansinių ir kitų išteklių, reikalingų Įstaigos IS veiklai atkurti, įvykus ekstremaliai situacijai, naudojimą;

14.8. organizuoja ir užtikrina Įstaigos IS duomenų fizinę saugą, įvykus ekstremaliai situacijai;

14.9. organizuoja logistiką (žmonių, daiktų, įrangos vežimo organizavimas ir jų vežimas į numatytą saugią vietą);

14.10. esant poreikiui, organizuoja Įstaigos IS veiklai atkurti reikalingų prekių, paslaugų ir darbų įsigijimą;

14.11. prižiūri ir koordinuoja Įstaigos IS veiklos atkūrimą;

14.12. atlieka kitas Valdymo grupei pavestas funkcijas.

15. Valdymo grupei paskelbus ekstremalią situaciją ir įsigaliojus Valdymo planui, esant būtinybei parengiami ir išsiunčiami informaciniai pranešimai Įstaigos IS naudotojams, Įstaigos IS vartotojams, duomenų gavėjams ir teikėjams, viešosios informacijos skleidėjams, teisėsaugos institucijoms, nurodant kontaktinį asmenį bei jo kontaktus, kuris įgaliotas suteikti papildomą informaciją.

16. Veiklos atkūrimo grupė (toliau – Atkūrimo grupė) sudaroma iš Įstaigos IS priežiūrą atliekančių administratorių ir IT paslaugų tiekėjo atstovų pagal vykdomas veiklos atkūrimo funkcijas. Valdymo grupės nariai neturėtų būti ir Atkūrimo grupės nariais, nebent išskirtiniais atvejais kai yra žmogiškųjų išteklių trūkumas. Atkūrimo grupės sudėtis:

16.1. Infrastruktūros ir sistemų priežiūros skyriaus vedėjas (Atkūrimo grupės vadovas);

16.2. IS administratoriai;

16.3. Aptarnaujantys darbuotojai (teikiantys Įstaigos IS ir (arba) IT infrastruktūros priežiūros paslaugas) ir (arba) kiti išoriniai ekspertai (pagal poreikį);

16.4. IT paslaugų teikėjo atstovas.

17. Atkūrimo grupė atlieka šias funkcijas:

17.1. organizuoja tarnybinių stočių veiklos atkūrimą;

17.2. organizuoja kompiuterių tinklo veikimo atkūrimą;

17.3. organizuoja Įstaigos IS informacijos atkūrimą;

17.4. organizuoja taikomųjų programų tinkamo veikimo atkūrimą;

17.5. organizuoja darbo kompiuterių veikimo atkūrimą ir prijungimą prie kompiuterių tinklo;

17.6. organizuoja ryšio su Įstaigos teritoriniais padaliniais ir kitomis įstaigomis, institucijomis ir kitomis organizacinėmis struktūromis atkūrimą;

17.7. atlieka kitas funkcijas ir veiksmus, būtinus Įstaigos IS veiklos atkūrimui.

18. Paskelbus ekstremalią situaciją Valdymo grupė ir Atkūrimo grupė organizuoja pasitarimus, įskaitant ir nuotoliniu būdu, bendrauja visomis tuo metu prieinamomis ryšio priemonėmis (telefonu, mobiliuoju ryšiu, elektroninių paštu). Esant poreikiui gali būti organizuojami bendri Valdymo grupės ir Atkūrimo grupės pasitarimai.

19. Atkūrimo grupės vadovas ne rečiau kaip 2 kartus per dieną informuoja Valdymo grupės vadovą ir narius apie jiems priskirtų funkcijų vykdymo eigą.

20. Paskelbus ekstremalią situaciją, siekiant atkurti Įstaigos IS veiklą, prireikus gali būti naudojamos atsarginės patalpos, kurių adresas ir būdai, kaip iki jų nuvykti nurodomi Valdymo plano 3 priede.

21. Atsarginėms patalpoms, naudojamoms Įstaigos IS veiklai atkurti, paskelbus ekstremalią situaciją, keliami šie reikalavimai:

21.1. Atsarginės patalpos turi būti fiziškai apsaugotos nuo neautorizuoto patekimo į jas. Jos turi būti įrengtos atskiroje rakinamoje patalpoje. Patalpų durys turi būti šarvuotos ir apsaugotos bent dviem skirtingos konstrukcijos spynomis;

21.2. Patekimas į patalpas turi būti registruojamas žurnale;

21.3. Patalpos turi atitikti priešgaisrinės saugos reikalavimus ir higienos reikalavimus, jose turi būti įrengtos gaisro gesinimo priemonės bei veikianti oro temperatūros ir drėgmės reguliavimo įranga (oro vėdinimo ir kondicionavimo sistema);

21.4. Atsarginės patalpos turi turėti nuolatinį elektros energijos ir interneto ryšį, taip pat turi būti įrengtas rezervinis elektros energijos šaltinis, užtikrinantis įrangos veikimą ne trumpiau kaip 30 minučių;

21.5. Ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo.

22. Detalusis planas, su nurodytais veiksmais ir jų vykdymo eiliškumu, terminais, atsakingais vykdytojais įvykus skirtingo pobūdžio elektroninės informacijos saugos incidentams, pateiktas Valdymo plano 4 priede. Už Detaliojo plano parengimą ir atnaujinimą atsakingas Saugos įgaliotinis kartu su Įstaigos IS administratoriais.

23. Ekstremali situacija yra atšaukiama kai:

23.1. pašalinamos priežastys sukėlusios ekstremalią situaciją;

23.2. atkuriamas Įstaigos IS veikimas, būtinas Įstaigos funkcijų vykdymui.

24. Atšaukus ekstremalią situaciją Užimtumo tarnybos direktoriaus paskirtas asmuo įvertina Valdymo grupės ir Atkūrimo grupės veikla ekstremalios situacijos metu, pateikiamos išvados ir siūlymai dėl Valdymo plano tobulinimo ar keitimo.

25. Saugos įgaliotinis yra atsakingas už Įstaigos IS naudotojų supažindinimą su Valdymo planu.

III SKYRIUS
APRAŠOMOSIOS NUOSTATOS

26. Įstaigos IS veiklos tęstinumui užtikrinti turi būti parengti šie dokumentai:

26.1. Įstaigos IS projektinė dokumentacija (IS specifikacijos), kurioje turi būti nurodyta konkrečių Įstaigos IS informacinių technologijų įranga ir jos parametrai;

26.2. už konkrečios informacinių technologijų įrangos priežiūrą atsakingų administratorių sąrašas bei minimalus Įstaigos IS veiklai atkurti nesant administratoriaus, kuris dėl komandiruotės, ligos ar kitų priežasčių negali operatyviai atvykti į darbo vietą, reikiamos kompetencijos ar žinių lygis (kuris negali būti žemesnis už Įstaigos IS administratoriui keliamų reikalavimų lygį);

26.3. patalpų, kuriose yra Įstaigos IS įranga, brėžiniai ir patalpose esančios įrangos bei komunikacijų sąrašas (tarnybinės stotys, kompiuterių tinklo ir telefonų tinklo mazgai bei šių tinklų vedimo tarp aukštų vietos, elektros įvedimo pastate vietos);

26.4. IS kompiuterinio tinklo fizinio ir loginio sujungimo schemos;

26.5. elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių sąrašas bei atsakingi už šių sutarčių įgyvendinimo priežiūrą asmenys;

26.6. dokumentas, kuriame nurodyta programinės įrangos laikmenų ir laikmenų su atsarginėmis elektroninės informacijos kopijomis saugojimo vieta ir šių laikmenų perkėlimo į saugojimo vietą laikas ir sąlygos;

26.7. Valdymo grupės ir Atkūrimo grupės narių sąrašai su kontaktiniais duomenimis, leidžiančiais susisiekti su šių grupių nariais bet kurio metu;

26.8. Už Valstybės duomenų centre esančios ir Įstaigos IS veikimui užtikrinti reikalingos įrangos techninės dokumentacijos parengimą ir atnaujinimą atsakingas IT paslaugų tiekėjas kartu su Infrastruktūros ir sistemų priežiūros skyriaus vedėju. Šios IT paslaugos teikiamos pagal paslaugų teikimo sutartį, sudarytą tarp Užimtumo tarnybos ir IT paslaugų teikėjo.

27. Už nurodytų dokumentų parengimą, reguliarų peržiūrėjimą ir atnaujinimą atsakingas Saugos įgaliotinis.

28. Už nurodytų dokumentų saugojimą atsakingi Įstaigos IS administratoriai. Atspausdinti dokumentai saugomi Įstaigos IS administratoriams prieinamoje vietoje.

IV SKYRIUS
PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

29. Valdymo plano veiksmingumas turi būti išbandomas ne rečiau kaip kartą per metus arba įvykus didesniems Įstaigos IS ar infrastruktūros pokyčiams. Išbandymo data nustatoma ne vėliau kaip iki kiekvienų metų vasario mėnesio paskutinės dienos.

30. Valdymo plano veiksmingumas turi būti atliekamas pagal sukurtą ekstremalios situacijos scenarijų, atsižvelgiant į per praėjusius metus įvykusius elektroninės informacijos saugos incidentus.

31. Valdymo plano veiksmingumo išbandymo metu:

31.1. imituojamos Incidentų situacijos, atsakingi Incidento valdymo ir pasekmių likvidavimo vykdytojai atlieka incidento situacijos metu būtinus atlikti veiksmus;

31.2. iš atsarginių duomenų kopijose esamų duomenų vykdomas Įstaigos IS informacijos ir duomenų atkūrimas.

32. Atlikus Valdymo plano veiksmingumo išbandymą, Saugos įgaliotinis per 14 kalendorinių dienų parengia Valdymo Plano veiksmingumo išbandymo ataskaitą (Valdymo plano 5

priedas) (toliau – Ataskaita), kurioje yra apibendrinami atliktų bandymų rezultatai, akcentuojami pastebėti trūkumai. Ataskaita pateikiama Valdymo grupei. Atsižvelgiant į nustatytus trūkumus Saugos įgaliotinis pateikia Valdymo grupei pasiūlymus dėl Valdymo plano atnaujinimo ar pakeitimo.

33. Saugos įgaliotinis ne vėliau kaip per penkias darbo dienas nuo Ataskaitos patvirtinimo, pateikia Ataskaitos kopiją Nacionaliniam kibernetinio saugumo centrui.

34. Valdymo plano veiksmingumo išbandymo metu pastebėti trūkumai šalinami remiantis operatyvumo, veiksmingumo ir ekonomiškumo principais.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

35. Valdymo planas yra peržiūrimas vieną kartą per metus. Valdymo panas turi būti peržiūrimas po rizikos analizės ar informacinių technologijų saugos atitikties vertinimo atlikimo arba įvykus esminiams organizaciniams, sisteminiams ar kitiems pokyčiams Įstaigoje. Prireikus Valdymo planas turi būti tikslinamas ir derinamas su Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos, vadovaujantis Bendrųjų elektroninės informacijos saugos reikalavimų aprašu.

36. Įstaigos IS naudotojai, pažeidę šio Plano ir kitų veiklos tęstinumą reglamentuojančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____

Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų veiklos tęstinumo valdymo plano
1 priedas

UŽIMTUMO TARNYBOS PRIE LIETUVOS RESPUBLIKOS SOCIALINĖS APSAUGOS IR DARBO MINISTERIJOS INFORMACINIŲ SISTEMŲ ATKŪRIMO PRIORITETAI IR ATSAKOMYBĖ

Eil. Nr. (prioritetas)	**Informacinės sistemos ir IT Infrastruktūra**	**Asmuo, atsakingas už Įstaigos IS atkūrimą**
1	Įstaigos kompiuterių tinklo veikimo atkūrimas	Infrastruktūros ir sistemų priežiūros skyriaus vedėjas
2	Tarnybinių stočių veikimo atkūrimas	Infrastruktūros ir sistemų priežiūros skyriaus vedėjas
3	Duomenų bazių atkūrimas	Infrastruktūros ir sistemų priežiūros skyriaus vedėjas
4	LDB IS (*eDBirža*) veiklos atkūrimas	IT plėtros skyriaus vedėjas
5	Dokumentų valdymo sistema (*DocLogix*)	Infrastruktūros ir sistemų priežiūros skyriaus vedėjas
6	***Neteko galios nuo 2023-12-22***	
7	Užimtumo tarnybos elektroninio pašto sistemos veiklos atkūrimas	Infrastruktūros ir sistemų priežiūros skyriaus vedėjas
8	Interneto svetainės	IT plėtros skyriaus vedėjas
9	Kompiuterizuotų darbo vietų veikimo atkūrimas	Infrastruktūros ir sistemų priežiūros skyriaus vedėjas
10	PVS (*Bonus*) veiklos atkūrimas	Infrastruktūros ir sistemų priežiūros skyriaus vedėjas

_____

Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų veiklos tęstinumo valdymo plano
2 priedas

KIBERNETINIŲ INCIDENTŲ VALDYMO IR NACIONALINIO KIBERNETINIO SAUGUMO CENTRO INFORMAVIMO TVARKOS APRAŠAS

1. Kibernetinių incidentų valdymo ir Nacionalinio kibernetinio saugumo centro informavimo tvarkos aprašas reglamentuoja kibernetinių incidentų valdymo ir Nacionalinio kibernetinio saugumo centro informavimo apie IS įvykusius kibernetinius incidentus tvarką.

2. Veiklos tęstinumo valdymo grupė nustato ir priskiria Incidentą kibernetinio incidento grupei (grupėms) ir poveikio kategorijai pagal Nacionalinis kibernetinių incidentų valdymo plano priede pateiktus kriterijus.

3. Saugos įgaliotinis informuoja Nacionalinį kibernetinio saugumo centrą (toliau – NKSC) apie IS įvykusius:

3.1. didelio poveikio kibernetinius incidentus – nedelsiant, bet ne vėliau kaip per 1 valandą nuo jų nustatymo;

3.2. vidutinio poveikio kibernetinius incidentus – ne vėliau kaip per 4 valandas nuo jų nustatymo;

3.3. nereikšmingo poveikio kibernetinius incidentus – periodiškai kiekvieno kalendorinio mėnesio pirmą darbo dieną.

4. NKSC informuojamas apie didelio ar vidutinio poveikio kibernetinius incidentus kibernetinio saugumo subjekto pranešimu, kuriame nurodoma:

4.1. trumpas kibernetinio incidento apibūdinimas;

4.2. tikslus laikas, kada kibernetinis incidentas įvyko ir buvo nustatytas;

4.3. kibernetinio incidento šalinimo tvarka (nurodoma ar tai prioritetas, ar ne);

4.4. tikslus laikas, kada bus teikiama kibernetinio incidento tyrimo ataskaita.

5. Informuojant apie nereikšmingą kibernetinį incidentą pateikiama informacija apie kiekvienos grupės incidentų, įvykusių nuo paskutinio pranešimo pateikimo dienos, skaičių.

6. NKSC pateikiama incidento tyrimo ataskaita:

6.1. didelės reikšmės kibernetinio incidento valdymo būklę – ne vėliau kaip per 4 valandas nuo jo nustatymo ir ne rečiau kaip kas keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

6.2. vidutinės reikšmės kibernetinio incidento valdymo būklę – ne vėliau kaip per 24 valandas nuo jo nustatymo ir ne rečiau kaip kas dvidešimt keturias valandas atnaujintą informaciją, iki kibernetinis incidentas suvaldomas ar pasibaigia;

6.3. didelio ar vidutinio poveikio kibernetinių incidentų suvaldymą ar pasibaigimą – ne vėliau kaip per 4 valandas nuo jų suvaldymo ar pasibaigimo.

7. Didelės ir vidutinės reikšmės kibernetinio incidento tyrimo ataskaitoje nurodoma žinoma informacija:

7.1. kibernetinio incidento grupė (grupės) ir poveikio kategorija;

7.2. IS komponento, kuriame nustatytas kibernetinis incidentas, tipas (informacinė sistema, posistemė, elektroninių ryšių tinklas, tarnybinė stotis ir pan.);

7.3. kibernetinio incidento veikimo trukmė;

7.4. kibernetinio incidento šaltinis;

7.5. kibernetinio incidento požymiai;

7.6. kibernetinio incidento veikimo metodas;

7.7. galimos kibernetinio incidento pasekmės;

7.8. kibernetinio incidento poveikio pasireiškimo (galimo išplitimo) mastas;

7.9. kibernetinio incidento būsena (aktyvus, pasyvus);

7.10. priemonės, kuriomis kibernetinis incidentas nustatytas;

7.11. galimos kibernetinio incidento valdymo priemonės;

7.12. tikslus laikas, kada bus teikiama pakartotinė kibernetinio incidento tyrimo ataskaita.

8. Apie didelės ir vidutinės reikšmės kibernetinio incidento sustabdymą ir pašalinimą NKSC pranešama ne vėliau kaip per 8 valandas nuo kibernetinio incidento sustabdymo ir pašalinimo.

9. Apie kibernetinius incidentus NKSC informuojamas naudojantis Kibernetinio saugumo informaciniu tinklu, o nesant galimybės – NKSC nurodytais kontaktais (tel. 1843, el. p. cert@nksc.lt).

_____

Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų veiklos tęstinumo valdymo plano
3 priedas

ATSARGINIŲ PATALPŲ, NAUDOJAMŲ UŽIMTUMO TARNYBOS INFORMACINIŲ SISTEMŲ VEIKLAI ATKURTI, ĮVYKUS INCIDENTUI, ADRESAI IR TECHNINĖS INFRASTRUKTŪROS PERKĖLIMAS

1. IT paslaugų tiekėjas, užtikrina, kad Įstaigos IS techninė infrastruktūra būtų talpinama dviejuose valstybiniuose duomenų centruose:

Eil. Nr.	Valstybinio duomenų centro pavadinimas	Valstybinio duomenų centro valdytojas	Valstybinio duomenų centro adresas
1.	VDC-KVTC-G11	Biudžetinė įstaiga Kertinis valstybės telekomunikacijų centras	Gedimino pr. 11, Vilnius
2.	VDC-LRTC-DC2	Akcinė bendrovė Lietuvos radijo ir televizijos centras	Sausio 13-osios g. 10, Vilnius

2. IT paslaugų tiekėjas, užtikrina tinkamą Įstaigos IS veiklai atkurti techninės infrastruktūros perkėlimą į IT paslaugų tiekėjo atsargines patalpas, jeigu Valstybinių duomenų centrų infrastruktūros veikla nėra dubliuojama.

_____

Užimtumo tarnybos prie Lietuvos Respublikos
socialinės apsaugos ir darbo ministerijos informacinių
sistemų veiklos tęstinumo valdymo plano
4 priedas

UŽIMTUMO TARNYBOS INFORMACINIŲ SISTEMŲ VEIKLOS ATKŪRIMO DETALUSIS PLANAS

Ekstremali situacija	Veiklos atkūrimo veiksmai	Atsakingi vykdytojai
Gautas pranešimas apie Incidentą, galintį įtakoti ekstremalios situacijos atsiradimą (pvz., virusą Įstaigos kompiuteriniame tinkle, patalpų pažeidimus, Techninės įrangos gedimus, darbuotojų nepasiekiamumą ir pan.)	Informuojama Veiklos tęstinumo valdymo grupė apie Incidentą	Saugos įgaliotinis
	Vykdomas informacijos rinkimas ir Incidento analizė (surenkama informacija iš IS tvarkytojų ir IS administratorių apie sutrikusių Įstaigos IS veiklą, patalpas arba patirtą kitokią žalą)	Valdymo grupė IS administratorius
	Skelbiama ekstremali situacija (jei pranešimas apie Incidentą patvirtinamas)	Valdymo grupės vadovas
	Prireikus parengiami ir išplatinami informaciniai pranešimai visiems naudotojams. Pranešime turi būti pateikiamos rekomendacijos, kaip elgtis esant ekstremaliai situacijai, nurodomi atsakingi darbuotojai ir jų kontaktinė informacija; taip pat išplatinami pranešimai IS tvarkytojams, duomenų gavėjams; viešosios informacijos skleidėjams; teisėsaugos institucijoms. Parengiamas priemonių planas kilusiam pavojui užkirsti. Sudaroma Veiklos atkūrimo grupė, atsižvelgiant į tai, kokios Įstaigos IS pažeistos bei pažeidimų pobūdį.	Valdymo grupė
1. Įstaigos patalpų pažeidimas arba praradimas (pvz., dėl gaisro, patalpų užpuolimo, pavojingų medžiagų patalpose, patalpų pažeidimo arba praradimo,	1.1. Informuojamos atitinkamos tarnybos ir institucijos (Priešgaisrinės apsaugos ir gelbėjimo tarnyba, Policija ir pan.). Evakuojami darbuotojai ir atliekami kiti veiksmai pagal įstaigoje patvirtintą ekstremalių situacijų valdymo planą.	Įstaigos darbuotojas atsakingas už darbuotojų saugą IT paslaugų teikėjas
	1.2. Įvertinama, ar kyla pavojus nepertraukiamai Įstaigos IS veiklai. Jei taip, toliau vykdomi veiksmai, numatyti 1.3 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 1.9 papunktyje.	Valdymo grupė IT paslaugų teikėjas

stichinės nelaimės, oro sąlygų, avarijų, karo veiksmų)	1.3. Įvertinama, ar reikia išjungti Įstaigos IS, kitas komunikcijas, galinčias kelti pavojų (elektros, valdentiekio ir pan.). Jei taip, toliau vykdomi veiksmai, numatyti 1.4 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 1.5 papunktyje.	Valdymo grupė IT paslaugų teikėjas
	1.4. Jei reikia, išjungiamos Įstaigos IS (jei yra galimybės, gali būti vykdoma nuotoliniu būdu), atjungiamos kitos komunikacijos.	Atkūrimo grupė IS administratorius Turto valdymo skyriaus atsakingas darbuotojas IT paslaugų teikėjas
	1.5. Įvertinama, ar pasiekiamas Įstaigos duomenų centras. Jei taip, toliau vykdomi veiksmai, numatyti 1.6 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti pagal 2 situaciją.	IT paslaugų teikėjas Atkūrimo grupė
	1.6. Priimamas sprendimas, ar reikia atkurti Įstaigos IS. Jei taip, toliau vykdomi veiksmai, numatyti 1.7 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 1.8 papunktyje.	Valdymo grupė
	1.7. Atkuriamos Įstaigos IS pagal numatytą prioritetą	Atkūrimo grupė IS administratorius
	1.8. Įvertinama, ar reikia imtis papildomų priemonių. Jei ne, laikoma, kad Įstaigos IS veikla atkurta. Jei taip, toliau vykdomi veiksmai, numatyti 1.9 papunktyje.	Valdymo grupė
	1.9. Pagal situaciją taikomos papildomos priemonės	Atkūrimo grupė IS administratorius
	1.10. Informuojami darbuotojai apie patalpų pasiekiamumą, kai gaunama informacija, kad patalpos tinkamos naudoti.	Įstaigos darbuotojas atsakingas už darbuotojų saugą IT paslaugų teikėjas
2. Nepasiekiamas pagrindinis Įstaigos duomenų centras (dėl gaisro pastato dalyje, kurioje yra duomenų centras, dėl inžinerinių	2.1. Nustatoma, kad nepasiekiamas pagrindinis duomenų centras.	Atkūrimo grupė IS administratorius IT paslaugų teikėjas
	2.2. Įvertinama, ar reikia atkurti Įstaigos IS atsarginiame duomenų centre. Jei taip, toliau vykdomi veiksmai, numatyti 2.3 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 2.4 papunktyje.	Valdymo grupė IT paslaugų teikėjas

sistemų gedimo (rezervinės elektros maitinimo, kondicionavimo ir vėdinimo ir pan.)	2.3. Vykdomas Įstaigos IS atkūrimas atsarginėse patalpose. Toliau vykdomi veiksmai, numatyti 2.4. punkte.	Atkūrimo grupė IT paslaugų teikėjas
	2.4. Įvertinama, ar reikia imtis papildomų priemonių. Jei taip, toliau vykdomi veiksmai, numatyti 2.5 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 2.6 papunktyje.	Valdymo grupė
	2.5. Pagal situaciją taikomos papildomos priemonės.	Atkūrimo grupė
	2.6. Įvertinama, ar galima grįžti į pagrindinį Įstaigos duomenų centrą. Jei ne, toliau vykdomi veiksmai, numatyti 2.4 papunktyje. Jei taip, toliau vykdomi veiksmai, numatyti 2.7 papunktyje.	Valdymo grupė
	2.7. Esant galimybei vykdomas Įstaigos IS atkūrimas pagrindiniame duomenų centre.	Atkūrimo grupė IS administratorius
	2.8. Atkūrus IS veikimą pagrindiniame duomenų centre priimamas sprendimas, kad Įstaigos IS veikla atkurta.	Valdymo grupė
3. Nepasiekiama techninė ar programinė įranga (dėl techninės įrangos gedimo, neturint rezervinės įrangos, kai nepavyko atkurti Įstaigos IS veikimo per 2 val. po įvykio ir nustatoma, kad to nepavyks padaryti teisės aktuose nustatytais terminais)	3.1. Nustatoma, kad nepasiekiama techninė ar programinė įranga.	Atkūrimo grupė IS administratorius
	3.2. Situacijos vertinimas, jei reikia, draudimo įmonės, kitų institucijų informavimas.	Valdymo grupė
	3.3. Įvertinama, ar Įstaiga turi pakankamai techninių resursų funkcijų perkėlimui. Jei taip, toliau vykdomi veiksmai, numatyti 3.4 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 3.5 papunktyje.	Valdymo grupė
	3.4. Funkcijos perkeliamos į laisvus resursus. Toliau vykdomi veiksmai, numatyti 3.5 papunktyje.	Atkūrimo grupė
	3.5. Įvertinama, ar pasiekiamas pagrindinis duomenų centras. Jei ne, toliau vykdomi veiksmai, numatyti pagal 2 situaciją. Jei taip, toliau vykdomi veiksmai, numatyti 3.6 papunktyje.	Valdymo grupė
	3.6. Įvertinama, ar reikia įsigyti papildomos techninės ar programinės įrangos arba yra galimybė atstatyti programinę įrangą iš atsarginių kopijų. Jei taip, toliau vykdomi veiksmai, numatyti 3.7 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 3.8 papunktyje.	Valdymo grupė

	3.7. Organizuojamas ir vykdomas papildomos techninės įrangos įsigijimas/nuoma arba sugadintos programinės įrangos atstatymas iš atsarinių kopijų.	Atkūrimo grupė IS administratorius
	3.8. Įvertinama, ar reikia imtis papildomų priemonių. Jei taip, toliau vykdomi veiksmai, numatyti 3.9 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 3.10 papunktyje.	Valdymo grupė
	3.9. Pagal situaciją taikomos papildomos priemonės.	Atkūrimo grupė
	3.10. Įvertinama, ar Įstaigos IS veikimas atkurtas, priimamas sprendimas, kad funkcijos atkurtos.	Valdymo grupės vadovas
4. Nepasiekiami ar sugadinti duomenys (kai pažeistas duomenų bazės integralumas, sugadinti duomenys atsarginėse kopijose, dėl kenksmingos programinės įrangos, dėl elektromagnetinio poveikio)	4.1. Nustatoma, kad duomenys nepasiekiami.	Valdymo grupė
	4.2. Įvertinama, ar reikia atkurti techninę įrangą. Jei taip, toliau vykdomi veiksmai pagal 3 situaciją. Jei ne, toliau vykdomi veiksmai, numatyti 4.3 papunktyje.	Valdymo grupė
	4.3. Įvertinama, ar yra informacijos atsarginės kopijos. Jei taip, toliau vykdomi veiksmai, numatyti 4.4 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 4.5 papunktyje.	Valdymo grupė
	4.4. Vykdomas duomenų atstatymas iš atsarginių kopijų.	Atkūrimo grupė IS administratorius
	4.5. Įvertinama, ar reikia atsatyti duomenis iš kitų šaltinių (pvz. suvesti duomenis rankiniu būdu, importuoti iš kitų šaltinių). Jei taip, toliau vykdomi veiksmai, numatyti 4.6 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 4.7 papunktyje.	Valdymo grupė
	4.6. Vykdomas duomenų atstaymas iš kitų šaltinių (suvedimas rankiniu būdu, importavimas iš kitų šaltinių ir pan.).	Atkūrimo grupė
	4.7. Įvertinama, ar reikia imtis papildomų priemonių Jei taip, toliau vykdomi veiksmai, numatyti 4.8 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 4.9 papunktyje.	Valdymo grupė
	4.8. Pagal situaciją taikomos papildomos priemonės.	Atkūrimo grupė
	4.9. Įvertinama, ar duomenys pasiekiami, ar jų vientisumas atstatytas, jei taip, priimamas sprendimas kad duomenys pasiekiami.	Valdymo grupė

5. Ryšio sutrikimai (dėl dingusio ryšio su paslaugų tiekėju (interneto), optinių kabelių nutrūkimas, neveikia sąsajos su išorinėmis sistemomis, dėl kibernetinių atakų)	5.1. Nustatoma ryšio sutrikimas (dingo ir (arba) nepasiekiamas). Atliekamas ryšio įrangos Įstaigoje patikrinimas	IS administratorius
	5.2. Situacijos analizė ir naudotojų informavimas apie sutrikimus kitais prieinamais kanalais.	Valdymo grupė
	5.3. Ryšio paslaugų teikėjo informavimas apie sutrikimus ir informacijos dėl sutrikimo trukmės ir pašalinimo prognozės įvertinimas.	Atkūrimo grupės vadovas
	5.4. Įvertinama, ar reikia organizuoti alternatyvius ryšio kanalus ar alternatyvias ryšio priemones. Jei taip, toliau vykdomi veiksmai, numatyti 5.5 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 5.6 papunktyje.	Valdymo grupė
	5.5. Alternatyvių ryšio priemonių organizavimas (pvz., ryšio paslaugų įsigijimo iš kito tiekėjo organizavimas, alternatyčių ryšio kanalų pajungimas ar pan.).	Atkūrimo grupė IS administratorius
	5.6. Įvertinama, ar reikia imtis papildomų priemonių. Jei taip, toliau vykdomi veiksmai, numatyti 5.7 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 5.8 papunktyje.	Valdymo grupė
	5.7. Pagal situaciją taikomos papildomos priemonės.	Atkūrimo grupė
	5.8. Įvertinama, ar yra atkurtas ryšio paslaugų teikimas, jei taip, priimamas sprendimas, kad ryšio paslaugos atkurtos.	Valdymo grupės vadovas
6. Elektros energijos tiekimo sutrikimas	6.1. Nustatoma, kad sutriko elektros energijos tiekimas. Atliekamas Įstaigos įvadinių elektros energijos tiekimo įrenginių patikrinimas ir pirminis sutrikimo įvertinimas.	IS administratorius Turto valdymo skyriaus vedėjas
	6.2. Įvertinama, ar veikia nepertraukiamo maitinimo šaltiniai (UPS) ir ar reikia pradėti IS tarnybinių stočių ir kitos techninės įrangos saugų išjungimą. Jei taip, toliau vykdomi veiksmai, numatyti 6. 3 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 6.5 papunktyje	IS administratorius
	6.3. Atliekamas IS tarnybinių stočių ir kitos techninės įrangos saugus išjungimas.	IS administratorius

	6.4. Elektros tiekėjo informavimas apie elektros energijos sutrikimą ir informacijos dėl sutrikimo trukmės ir pašalinimo prognozės įvertinimas	Turto valdymo skyriaus vedėjas
	6.5. Dubliuoto elektros energijos tiekimo šaltinio organizavimas/paleidimas (elektros energijos tiekimo iš kito šaltinio orgalnizavimas: stacionaraus dyzelinio generatoriaus, mobilaus dyzelinio generatoriaus ar pan.)	Atkūrimo grupė IT paslaugų tiekėjas
	6.6. Situacijos analizė ir naudotojų informavimas apie elektros energijos tiekimo sutrikimus bei rekomendacijų pateikimas	Valdymo grupė
	6.7. Įvertinama, ar reikia imtis papildomų priemonių. Jei taip, toliau vykdomi veiksmai, numatyti 6.8 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 6.9 papunktyje.	Valdymo grupė
	6.8. Pagal situaciją taikomos papildomos priemonės.	Atkūrimo grupė
	6.9. Įvertinama, ar elektros energijos tiekėjas pašalino sutrikimo priežastis ir ar yra atkurtas elektros energijos tiekimas, jei taip, priimamas sprendimas, kad elektros energijos tiekimas atkurtas.	Valdymo grupė
7. Nepasiekiami darbuotojai (kai negali atvykti į darbą daugiau nei penktadalis darbuotojų dėl oro sąlygų, stichinių nelaimių, avarijų, epidemijų, mobilizacijos, cheminės atakos, karo veiksmų ir pan.)	7.1. Nustatoma, kad nepasiekiami darbuotojai (daugiau nei 20 proc.).	Valdymo grupė
	7.2. Vykdoma situacijos analizė.	Valdymo grupė
	7.3. Įvertinama, ar darbuotojai gali dirbti nuotoliniu būdu (pvz., iš namų), ar reikia samdyti išorinius paslaugų tiekėjus. Jei taip, toliau vykdomi veiksmai, numatyti 7.4 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 7.5 papunktyje.	Valdymo grupė
	7.4. Pagal situaciją darbuotojai vykdo savo funkcijas nuotoliniu būdu arba vykdomas išorinių paslaugų tiekėjų samdymas.	Atkūrimo grupė IS administratorius
	7.5. Įvertinama, ar darbuotojų nepasiekiamumas įtakoja Įstaigos veiklą ir (arba) paslaugų teikimą. Jei taip, toliau vykdomi veiksmai, numatyti 7.6 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 7.7 papunktyje.	Valdymo grupė
	7.6. parengiami ir išplatinami informaciniai pranešimai visiems naudotojams, duomenų gavėjams ir kitiems suinteresuotiesiems asmenims apie galimus paslaugų teikimo sutrikimus.	Atkūrimo grupė

	7.7. Įvertinama, ar reikia imtis papildomų priemonių. Jei taip, toliau vykdomi veiksmai, numatyti 7.8 papunktyje. Jei ne, toliau vykdomi veiksmai, numatyti 7.9 papunktyje.	Valdymo grupė
	7.8. Pagal situaciją taikomos papildomos priemonės.	Atkūrimo grupė
	7.9. Darbuotojai paslaugas teikia nuotoliniu būdu arba naudojamasi išorinių paslaugų tiekėjų paslaugomis kol pašalinamos priežastys, įtakojusios darbuotojų nepasiekiamumą.	Valdymo grupės vadovas

_____

Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų veiklos tęstinumo valdymo plano
5 priedas

(Užimtumo tarnybos informacinių sistemų veiklos tęstinumo valdymo plano veiksmingumo išbandymo ataskaitos pavyzdinė forma)

UŽIMTUMO TARNYBOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO ATASKAITA

(Valdymo grupės posėdžio data, dokumento numeris ir vieta)

Ekstremalios situacijos bandyme dalyvavo:

1. _____
2. _____
3. _____
...

Trumpas ekstremalios situacijos scenarijaus aprašymas:

_____

_____

_____

Įstaigos IS komponentai, kuriuos paveikė ekstremali situacija:

_____

_____

_____

Ekstremalios situacijos valdymo eiga:

_____

_____

_____

Nustatyti Įstaigos IS veiklos tęstinumo valdymo ar veiklos atkūrimo detaliojo plano trūkumai:

_____

_____

_____

Siūlymai ir rekomendacijos dėl Įstaigos informacinių sistemų veiklos tęstinumo valdymo plano keitimo:

_____

_____

_____

(vardas, pavardė)	(parašas)
(vardas, pavardė)	(parašas)

Priedo pakeitimai:
Nr. V-252, 2023-12-21, paskelbta TAR 2023-12-21, i. k. 2023-24884

Priedo pakeitimai:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

1 priedas. *Neteko galios nuo 2022-09-28*
Priedo naikinimas:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

2 priedas. *Neteko galios nuo 2022-09-28*
Priedo naikinimas:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

3 priedas. *Neteko galios nuo 2022-09-28*
Priedo naikinimas:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

4 priedas. *Neteko galios nuo 2022-09-28*
Priedo naikinimas:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

5 priedas. *Neteko galios nuo 2022-09-28*
Priedo naikinimas:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

Patvirtinta. *Neteko galios nuo 2022-09-28*
Priedo naikinimas:
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565

Pakeitimai:

1.
Užimtumo tarnyba prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos, Įsakymas
Nr. V-298, 2022-09-27, paskelbta TAR 2022-09-27, i. k. 2022-19565
Dėl Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus 2021 m. kovo 19 d. įsakymo Nr. V-113 „Dėl Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų duomenų saugos nuostatų ir elektroninės informacijos saugos politiką įgyvendinančių dokumentų patvirtinimo“ pakeitimo

2.
Užimtumo tarnyba prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos, Įsakymas
Nr. V-252, 2023-12-21, paskelbta TAR 2023-12-21, i. k. 2023-24884
Dėl Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos direktoriaus 2021 m. Kovo 19 d. įsakymo Nr. V-113 „Dėl Užimtumo tarnybos prie Lietuvos Respublikos socialinės apsaugos ir darbo ministerijos informacinių sistemų duomenų saugos nuostatų ir elektroninės informacijos saugos politiką įgyvendinančių dokumentų patvirtinimo“ pakeitimo