PATVIRTINTA
Lietuvos Respublikos Vyriausybės
2024 m. gegužės 15 d.
nutarimu Nr. 349
(Lietuvos Respublikos Vyriausybės
2024 m. d. nutarimo Nr.
redakcija)

VALSTYBĖS INFORMACINIŲ IŠTEKLIŲ IR JŲ KOPIJŲ LAIKYMO DUOMENŲ CENTRUOSE IR ŠIŲ IŠTEKLIŲ VEIKLOS ATKŪRIMO IŠ KOPIJŲ TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybės informacinių išteklių ir jų kopijų laikymo duomenų centruose ir šių išteklių veiklos atkūrimo iš kopijų tvarkos aprašas (toliau – Aprašas) nustato:

1.1. valstybės informacinių išteklių (toliau – VII) laikymo valstybiniuose duomenų centruose (toliau – VDC) tvarką;

1.2. VII, kurie turi būti prieinami karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais (toliau – kritiniai VII), kopijų laikymo kitose Europos Sąjungos valstybėse narėse, Europos ekonominės erdvės valstybėse ir (arba) Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse (toliau – ES ir (arba) NATO valstybės) esančiuose duomenų centruose ir šių VII veiklos atkūrimo iš kopijų tvarką;

1.3. informacinių sistemų ir jose tvarkomų duomenų, kai vidutinės svarbos ir mažos svarbos VII laikomi Lietuvos Respublikoje ar ES ir (arba) NATO valstybėse esančiuose privačiuose juridinių asmenų valdomuose duomenų centruose (toliau – privatūs DC), kopijų laikymo VDC ir šių VII veiklos atkūrimo iš kopijų tvarką;

1.4. informacinių sistemų ir jose tvarkomų duomenų, kai ypatingos svarbos ir svarbūs VII pagal atskirą Lietuvos Respublikos Vyriausybės nutarimą laikomi ES ir (arba) NATO valstybėse esančiuose privačiuose DC, kopijų laikymo VDC ir šių VII veiklos atkūrimo iš kopijų tvarką;

1.5. Aprašo 1.1–1.4 papunkčiuose nurodytų VII sudarančių informacinių sistemų ir jose tvarkomų duomenų kopijų parengimo ir perdavimo į duomenų centrus (toliau – DC) reikalavimus;

1.6. vidutinės svarbos ir mažos svarbos VII, laikomų Lietuvos Respublikos ar ES ir (arba) NATO valstybių teritorijoje esančiuose privačiuose DC, ypatingos svarbos ir svarbių VII, kurie pagal atskirą Vyriausybės nutarimą laikomi ES ir (arba) NATO valstybių teritorijoje esančiuose privačiuose DC, (toliau kartu – kiti VII) ir kritinių VII veiklos atkūrimo iš kopijų reikalavimus.

2. Aprašas parengtas vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 10 straipsnio 3 punktu ir 45 straipsnio 2–5 dalimis.

3. Aprašo nuostatos taikomos Valstybės informacinių išteklių valdymo įstatymo 2 straipsnio 46 dalyje nurodytiems subjektams (toliau – subjektai).

4. VII kopija (angl. *Cold copy*) Apraše suprantama kaip VII sudarančių duomenų ir jiems tvarkyti skirtos programinės įrangos (toliau – Programinė įranga) kopija, kuri daroma sustabdžius duomenų tvarkymui naudojamos Programinės įrangos veikimą ir yra naudojama Programinei įrangai ir (ar) duomenims atkurti tuo atveju, kai to nebegalima padaryti jokiomis kitomis priemonėmis ir (ar) iš tos Programinės įrangos ar duomenų rezervinių kopijų. Programinė įranga į

VII kopiją gali būti neįtraukiama tik tuo atveju, jei ji naudojama kaip privataus paslaugų teikėjo teikiama paslauga (angl. *SaaS* arba *PaaS*) ir nėra techninių galimybių ją įtraukti į VII kopiją.

5. Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos ir vartojamos Lietuvos Respublikos dokumentų ir archyvų įstatyme, Lietuvos Respublikos elektroninių ryšių įstatyme, Lietuvos Respublikos karo padėties įstatyme, Lietuvos Respublikos kibernetinio saugumo įstatyme ir jį įgyvendinančiuose teisės aktuose, Lietuvos Respublikos krizių valdymo ir civilinės saugos įstatyme, Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme, Lietuvos Respublikos nepaprastosios padėties įstatyme, Lietuvos Respublikos oficialiosios statistikos ir valstybės duomenų valdysenos įstatyme, Lietuvos Respublikos teisės gauti informaciją ir duomenų pakartotinio naudojimo įstatyme, Valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos valstybės tarnybos įstatyme, Lietuvos Respublikos valstybės ir savivaldybių turto valdymo, naudojimo ir disponavimo juo įstatyme, Lietuvos Respublikos viešojo administravimo įstatyme, Lietuvos Respublikos viešųjų pirkimų įstatyme.

II SKYRIUS
VII LAIKYMAS DC

6. Subjektai VDC laiko:

6.1. vidutinės ir (ar) mažos svarbos VII, kai tas pats subjektas valdo ir ypatingos svarbos ir (ar) svarbius VII;

6.2. ypatingos svarbos ir (ar) svarbius VII, kai, vadovaujantis Valstybės informacinių išteklių valdymo įstatymo 45 straipsnio 3 dalimi, subjektui pagal atskirą Vyriausybės nutarimą nėra suteikta teisė laikyti jo valdomų ypatingos svarbos ir svarbių valstybės informacinius išteklių privačiuose DC;

6.3. į Vyriausybės tvirtinamą kritinių VII sąrašą įtrauktus VII;

6.4. vidutinės ir (ar) mažos svarbos VII, kai juos valdantys subjektai yra įtraukti į Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“.

7. VII privačiuose DC laikomi, kai, vadovaujantis Valstybės informacinių išteklių valdymo įstatymo 45 straipsnio 3 dalimi, subjektui atskiru Vyriausybės nutarimu suteikta teisė laikyti jo valdomus ypatingos svarbos ir svarbius valstybės informacinius išteklius privačiuose DC, o šių VII kopijos Aprašo III skyriuje nustatyta tvarka laikomos VDC.

8. Subjektai, neįtraukti į Saugiojo valstybinio duomenų perdavimo tinklo naudotojų sąrašą, valdomus vidutinės ir (ar) mažos svarbos VII turi teisę laikyti arba VDC, arba privačiuose DC, o šių VII kopijos Aprašo III skyriuje nustatyta tvarka laikomos VDC.

9. Visų rūšių VII, kuriuos sudaro ir asmens duomenys, laikant už Europos ekonominės erdvės ribų esančiose Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse, turi būti vadovaujamasi 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) V skyriuje nustatytais reikalavimais.

10. Tais atvejais, kai VII valdytojai yra subjektai, įtraukti į Vyriausybės nutarimu, kuriuo patvirtintas Aprašas, (toliau – Nutarimas) patvirtintą Valstybės institucijų ir įstaigų, gaunančių centralizuotai teikiamas informacinių technologijų paslaugas, sąrašą (toliau – Sąrašas), jų

valdomų VII laikymo VDC arba privačiame DC paslaugą pagal IT paslaugų teikimo sutartį teikia Nutarimo 4.1 papunktyje nurodytas valstybės IT paslaugų teikėjas, išskyrus atvejus, kai subjektai valdomos informacinės sistemos veikimui užtikrinti naudoja programinę įrangą, kuri yra naudojama kaip privataus paslaugų teikėjo teikiama paslauga (angl. *SaaS*).

III SKYRIUS
VII KOPIJŲ LAIKYMAS DC

11. Tuo atveju, kai kritinių VII kopijoms laikyti yra naudojami privatūs DC, šie DC turi būti ne Lietuvos Respublikoje, o tose ES ir (ar) NATO valstybėse, kurios nesiriboja su valstybėmis, įtrauktomis į Valstybių ar teritorijų, kurių tiekėjai, jų subtiekėjai, ūkio subjektai, kurių pajėgumais yra remiamasi, gamintojai, techninės ar programinės įrangos priežiūrą ir palaikymą vykdantys asmenys ar juos kontroliuojantys asmenys nelaikomi patikimais, sąrašą, patvirtintą Lietuvos Respublikos Vyriausybės 2022 m. kovo 30 d. nutarimu Nr. 280 „Dėl Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 13–15 dalių nuostatų įgyvendinimo“ (toliau – Nesiribojančios valstybės).

12. Kritinių VII, jeigu juos sudaro ir asmens duomenys, kopija saugoma Šiaurės Atlanto sutarties organizacijos (NATO) valstybėse narėse esančiuose privačiuose DC, laikantis Reglamento (ES) 2016/679 nustatytų reikalavimų, įskaitant nustatytus Reglamento (ES) 2016/679 V skyriuje. Jeigu Europos Komisija nėra priėmusi sprendimų, jog už Europos ekonominės erdvės ribų esančios Šiaurės Atlanto sutarties organizacijos (NATO) valstybės užtikrina tinkamo lygio apsaugą, tuomet jose esančiuose duomenų centruose talpinant asmens duomenis, be kitų Reglamento (ES) 2016/679 reikalavimų, privaloma taikyti vieną iš Reglamento (ES) 2016/679 46 straipsnyje nurodytų apsaugos priemonių.

13. Kritinių VII kopijoms laikyti Nesiribojančių valstybių teritorijose esančių privačių DC nuomos ar juose esančios reikalingos informacinių technologijų infrastruktūros nuomos paslaugos įsigyjamos Viešųjų pirkimų įstatymo nustatyta tvarka.

14. Viešųjų pirkimų sutartys (toliau – Sutartis) dėl Nesiribojančių valstybių teritorijose esančių privačių DC nuomos ar juose esančios reikalingos informacinių technologijų infrastruktūros nuomos paslaugų kritinių VII kopijoms laikyti sudaromos tarp šių paslaugų teikėjų (toliau – Paslaugų teikėjas) ir paslaugų gavėjų. Sutartis dėl Valstybės skaitmeninių sprendimų agentūros centralizuotai teikiamomis IT paslaugomis besinaudojančių subjektų valdomų kritinių VII kopijų laikymo Nesiribojančių valstybių teritorijose esančiuose privačiuose DC centralizuotai sudaro ir už jų įgyvendinimą atsako Valstybės skaitmeninių sprendimų agentūra, o Valstybės skaitmeninių sprendimų agentūros centralizuotai teikiamomis IT paslaugomis nesinaudojančių subjektų atvejais sutartis sudaro ir jas įgyvendina patys subjektai.

15. Tais atvejais, kai kitų VII valdytojai yra subjektai, įtraukti į Sąrašą, jų valdomų kitų VII kopijų laikymo VDC paslaugą pagal IT paslaugų teikimo sutartį teikia Nutarimo 4.1 papunktyje nurodytas valstybės IT paslaugų teikėjas.

16. Tais atvejais, kai kritinių VII ir kitų VII valdytojai nėra subjektai, įtraukti į Sąrašą, paslaugų gavėjais laikomi patys kritinių VII ir kitų VII valdytojai arba šių VII tvarkytojai, kurie sudaro Sutartis dėl Nesiribojančių valstybių teritorijose esančių privačių DC nuomos ar juose esančios reikalingos informacinių technologijų infrastruktūros nuomos paslaugų kritinių VII kopijoms laikyti. Paslaugų teikėjais laikomi Nesiribojančių valstybių teritorijose esančių privačių DC nuomos ar juose esančios reikalingos informacinių technologijų infrastruktūros nuomos Paslaugų teikėjai, kurių paslaugos įsigyjamos Viešųjų pirkimų įstatymo nustatyta tvarka.

17. Tuo atveju, kai Sutartis dėl Nesiribojančių valstybių teritorijose esančių privačių DC nuomos ar juose esančios reikalingos informacinių technologijų infrastruktūros nuomos paslaugų kritinių VII kopijoms laikyti su Paslaugų teikėjais centralizuotai sudaro Valstybės skaitmeninių sprendimų agentūra, kuri laikoma paslaugų gavėja, kritinių VII valdytojai turi pasirašyti sutartis su Valstybės skaitmeninių sprendimų agentūra dėl informacinių technologijų paslaugų teikimo (toliau – IT paslaugų teikimo sutartis) ir pateikti jai užsakymą dėl kritinių VII kopijų laikymo Nesiribojančių valstybių teritorijose esančiuose privačiuose DC (toliau – Užsakymas). Teikdami Užsakymą Valstybės skaitmeninių sprendimų agentūrai, kritinių VII valdytojai privalo nurodyti konkretų kritinių VII kopijoms laikyti reikalingą saugyklos dydį ir pagrįsti pasirinkto dydžio saugyklos poreikį.

18. Siekiant užtikrinti tinkamą VII kopijų laikymą, paslaugų gavėjas, vadovaudamasis Kibernetinio saugumo įstatymo ir šio įstatymo įgyvendinamaisiais teisės aktais, privalo:

18.1. nustatyti paslaugų gavėjo ir Paslaugų teikėjo atsakomybes užtikrinant kibernetinį saugumą;

18.2. užtikrinti, kad Sutartyse būtų nurodoma paslaugų gavėjo ir Paslaugų teikėjo atstovų, atsakingų už kibernetinį saugumą, kontaktinė informacija (vardas, pavardė, mobiliojo ryšio telefono numeris, elektroninio pašto adresas);

18.3. nustatyti duomenų ar IT paslaugų vientisumo, prieinamumo ir konfidencialumo užtikrinimo reikalavimus;

18.4. nustatyti reikalavimus dėl IT paslaugų kontrolės ir paslaugų atitikties pirkimų sutartiniams reikalavimams auditavimo, susijusio su kibernetinio saugumo užtikrinimu;

18.5. nustatyti paslaugų perdavimo subteikėjams sąlygas;

18.6. nustatyti Programinės įrangos licencijavimo, kritinių VII kopijų turtinės ir intelektinės nuosavybės teisių užtikrinimo reikalavimus;

18.7. apibrėžti VII kopijos ir informacinių technologijų infrastruktūros apimtis;

18.8. nustatyti prieigos prie visų įvykių ir audito įrašų, susijusių su paslaugos gavėju ar jam teikiamomis paslaugomis, reikalavimus;

18.9. nustatyti paslaugų ar duomenų perkėlimo ar sunaikinimo reikalavimus;

18.10. nustatyti paslaugų teikimo nutraukimo reikalavimus, numatant ne mažesnį kaip 6 mėnesių laikotarpį, per kurį Paslaugų teikėjas turi pranešti paslaugų gavėjui apie paslaugų teikimo nutraukimą;

18.11. nustatyti prieigos prie duomenų suteikimo ir valdymo reikalavimus, nustatant pareigą Paslaugų teikėjui nedelsiant, bet ne vėliau kaip per vieną valandą nuo atsitiktinės ar neteisėtos prieigos prie duomenų, jų sunaikinimo, pakeitimo, sugadinimo ar kitokio neteisėto tvarkymo ar prieigos fakto, apie tai pranešti paslaugų gavėjui;

18.12. nustatyti dalijimosi tarp paslaugų gavėjo ir Paslaugų teikėjo informacija apie kibernetines grėsmes ir pažeidžiamumą reikalavimus;

18.13. nustatyti Paslaugų teikėjo techninės įrangos, Programinės įrangos, paslaugų testavimo reikalavimus;

18.14. nustatyti Paslaugų teikėjo veiklos tęstinumo, kibernetinių incidentų ir kitų nenumatytų atvejų valdymo reikalavimus;

18.15. apibrėžti pranešimo tarp paslaugų gavėjo ir Paslaugų teikėjo apie sutrikimus ir kibernetinius incidentus tvarkos ir sutrikimų bei kibernetinių incidentų valdymo tvarkos reikalavimus;

18.16. nustatyti Paslaugų teikėjo pareigas, siekiant užtikrinti atitiktį Reglamento (ES) 2016/679 28 straipsnio 3 dalies bei kitų asmens duomenų apsaugą reglamentuojančių teisės

aktų reikalavimams, Kibernetinio saugumo įstatymo ir jo įgyvendinamųjų teisės aktų reikalavimams, taip pat kitiems kibernetinį saugumą reglamentuojantiems teisės aktams;

18.17. tais atvejais, kai kritinių VII kopijos laikomos Nesiribojančių valstybių teritorijose esančiuose privačiuose DC, turi būti apibrėžti reikalavimai dėl regionų ar prieinamumo zonų, kuriose duomenys bus laikomi, keitimo – Paslaugų teikėjas neturi teisės be paslaugų gavėjo raštiško sutikimo pakeisti paslaugų teikimo regiono ar prieinamumo zonos.

19. Prieš sudarydamas Sutartį su Paslaugų teikėju, paslaugų gavėjas turi įvertinti Paslaugų teikėjo ir savo turimas kompetencijas, taikomas technines ir organizacines priemones, skirtas Aprašo 18 punkte nustatytiems reikalavimams vykdyti, ir su jų vykdymu susijusias rizikas:

19.1. užtikrinti asmens duomenų apsaugą, kibernetinio saugumą reglamentuojančių teisės aktų, sutartinių įsipareigojimų, veiklos standartų ir vidaus teisės aktų reikalavimus;

19.2. neperduoti Paslaugų teikėjui nuosavybės (įskaitant ir intelektinę nuosavybę) teisių į Paslaugų teikėjo laikomą kritinių VII kopiją;

19.3. užtikrinti kritinių VII veiklos tęstinumą ir pajėgumą atkurti kritinių VII veiklą tuo atveju, jeigu Paslaugų teikėjas prarastų jo laikomą kritinių VII kopiją ar iš šios kopijos nebūtų galimybės atkurti kritinių VII veiklos;

19.4. imtis priemonių, jeigu duomenys iš Paslaugų teikėjo infrastruktūroje laikomos VII kopijos būtų atsitiktiniai ar neteisėtai atskleisti, taip pat būtų kitaip pažeistas laikomų duomenų vientisumas, prieinamumas ir konfidencialumas;

19.5. valdyti prieigą prie Paslaugų teikėjo laikomų kritinių VII kopijų ir užtikrinti Paslaugų teikėjo laikomų kritinių VII kopijų prieinamumą;

19.6. per Sutartyje nustatytą laiką gauti iš Paslaugų teikėjo informaciją apie kibernetinio saugumo, duomenų vientisumo, prieinamumo ir konfidencialumo reikalavimų pažeidimus.

20. Kritinių VII kopijas laikant Nesiribojančių valstybių teritorijose esančiuose privačiuose DC, prieš sudarydamas Sutartį su Paslaugų teikėju, paslaugų gavėjas turi įvertinti riziką, susijusią su užsienio valstybės, kurioje veikia Paslaugų teikėjas, įstatymų taikymu, kuris gali turėti neigiamos įtakos Paslaugų teikėjo laikomoms kritinių VII kopijoms ir teikiamoms paslaugoms.

21. Sutarties su Paslaugų teikėju rizikos įvertinimo rezultatai išdėstomi VII rizikos įvertinimo ataskaitoje (toliau – rizikos įvertinimo ataskaita), kurią tvirtina paslaugų gavėjo vadovas. Vadovaudamasis rizikos įvertinimo ataskaita, paslaugų gavėjas parengia ir tvirtina rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, organizacinių, administracinių ir kitų išteklių poreikis rizikai valdyti. Jeigu rizikos įvertinimo ataskaitoje nustatyta rizika yra didelė, Sutartis su Paslaugų teikėju negali būti sudaryta, kol rizika nebus pašalinta.

22. Rizikos įvertinimo ataskaitas, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas paslaugų gavėjas ne vėliau kaip per penkias darbo dienas nuo šių dokumentų parengimo ar atnaujinimo dienos pateikia Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos, kuris per 20 darbo dienų nuo dokumentų gavimo dienos pateikia savo išvadą, ar sudaryti Sutartį su Paslaugų teikėju yra saugu.

23. Kai VII valdantys subjektai valdomus VII saugo privačiuose DC ir nesinaudojama valstybės IT paslaugų teikėjo teikiamomis IT paslaugomis, VII valdantiems subjektams rekomenduojama taikyti Aprašo 18–22 punktuose nustatytus reikalavimus VII ir (ar) jų kopijų saugojimo privačiuose DC paslaugoms. Papildomai turi būti nustatomas reikalavimas dėl šių VII kopijos perdavimo VDC.

IV SKYRIUS
VII IR JŲ KOPIJŲ PARENGIMO IR PERDAVIMO DC IR ŠIŲ KOPIJŲ LAIKYMO DC REIKALAVIMAI

24. Kritinių VII kopijos parengiamos ir į Nesiribojančių valstybių teritorijose esančius privačius DC ar VDC perduodamos, vadovaujantis Kibernetinio saugumo įstatymo ir jo įgyvendinamųjų teisės aktų reikalavimais.

25. Kritinių VII kopijos parengimą ir perdavimą Nesiribojančių valstybių teritorijose esantiems privatiems DC, o kitų VII kopijų perdavimą VDC vykdo VII valdytojas ar jo pavedimu kritinių VII tvarkytojas. Tuo atveju, kai kritinių VII ar kitų VII valdytojas ar tvarkytojas yra įtrauktas į Sąrašą, kritinių VII kopijos parengimą ir perdavimą Nesiribojančių valstybių teritorijose esantiems privatiems DC, o kitų VII kopijos perdavimą VDC, gavusi Užsakymą, pagal kompetenciją vykdo Valstybės skaitmeninių sprendimų agentūra.

26. Už tai, kad kritinių VII kopija būtų laiku parengta ir perduota Nesiribojančių valstybių teritorijose esantiems privatiems DC, o kitų VII kopija būtų perduota VDC atsako Aprašo 25 punkte nurodytas subjektas, kuris rengia atitinkamų VII kopijas.

27. Kritinių VII kopija parengiama ir Nesiribojančių valstybių teritorijose esantiems privatiems DC, o kitų VII kopija VDC perduodama tokiu dažnumu, kaip tai nustatyta kibernetinio saugumo politikos dokumentuose, kurie rengiami ir tvirtinami vadovaujantis Kibernetinio saugumo įstatymu ir jį įgyvendinančiais teisės aktais.

28. Aprašo Nesiribojančių valstybių teritorijose esančiuose privačiuose DC kritinių VII kopija laikoma 3 mėnesius nuo jos pirmosios dalies (pirminio elemento) patalpinimo minėtuose DC datos. VDC kitų VII kopija laikoma 3 mėnesius nuo jos pirminio elemento patalpinimo minėtuose DC datos.

29. Pasibaigus Aprašo 28 punkte nurodytiems terminams, Aprašo 25 punkte nurodytas subjektas, kuris rengia kritinių VII ar kitų VII kopiją ir perduoda ją Nesiribojančių valstybių teritorijose esantiems privatiems DC ar VDC, privalo ją sunaikinti.

30. Už kritinių VII kopijų, laikomų Nesiribojančių valstybių teritorijose esančiuose privačiuose DC, ar kitų VII kopijų, laikomų VDC, asmens duomenų apsaugą, kibernetinio saugumo reikalavimų įgyvendinimą bei apsaugą nuo neteisėtos prieigos ir neteisėto atkūrimo nuo jų perkėlimo į Nesiribojančių valstybių teritorijose esančius privačius DC ar VDC momento atsako paslaugų gavėjas, Paslaugų teikėjas, kritinių VII valdytojai ir tvarkytojai pagal sutartyse nustatytas atsakomybes.

31. Padarius kritinių VII kopijas ir patalpinus jas Nesiribojančių valstybių teritorijose esančiuose privačiuose DC, o kitų VII kopijas – VDC, kiekvieną kartą turi būti patikrinama, ar kritinių ar kitų VII kopijos suformavimas atliktas sėkmingai. Už kopijavimo proceso kontrolę ir kopijavimo proceso metu sugadintų kritinių VII ar kitų VII kopijų atkūrimą atsako Aprašo 25 punkte nurodytas subjektas, kuris vykdo kritinių VII ar kitų VII kopijos parengimą ir perdavimą Nesiribojančių valstybių teritorijose esantiems privatiems DC ar VDC. Įrašai apie kopijavimo atlikimą turi būti saugomi kopijų darymo sistemos įvykių žurnale.

32. Bent kartą per pusmetį nuo kritinių VII ar kitų VII duomenų kopijų patalpinimo Nesiribojančių valstybių teritorijose esančiuose privačiuose DC ar VDC dienos turi būti atliekamas testavimas, siekiant nustatyti, ar iš jų gali būti atkurti VII sudarantys duomenys ir informacinės sistemos. Šiame punkte nurodytą testavimą atlieka Aprašo 25 punkte nurodytas

subjektas, kuris vykdo kritinių VII ar kitų VII kopijos parengimą ir perdavimą Nesiribojančių valstybių teritorijose esantiems privatiems DC ar VDC.

V SKYRIUS
KRITINIŲ IR KITŲ VII VEIKLOS ATKŪRIMO IŠ KOPIJŲ UŽTIKRINIMO REIKALAVIMAI

33. Valstybės skaitmeninių sprendimų agentūra, gavusi Užsakymą, parengia kritinių VII kopijoms laikyti reikalingą informacinių technologijų infrastruktūrą Nesiribojančių valstybių teritorijose esančiuose privačiuose DC.

34. Tuo atveju, kai Sutartis su Paslaugų teikėjais centralizuotai sudaro Valstybės skaitmeninių sprendimų agentūra, kritinių VII valdytojai arba VII tvarkytojai, suderinę su VII valdytoju, ne vėliau kaip per 6 mėnesius nuo Užsakymo pateikimo dienos turi Valstybės skaitmeninių sprendimų agentūrai pateikti:

34.1. kritinių VII architektūros aprašymą ir nurodyti šių kritinių VII ryšius su kitais VII, taip pat pažymėti, kurie kritinių VII ryšiai su kitais VII yra būtini, siekiant atkurti kritinių VII veiklą iš VII kopijos karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitų krizių atvejais;

34.2. išsamias instrukcijas dėl kritinių VII veiklos iš kritinių VII kopijos, parengtos ir perduotos Nesiribojančių valstybių teritorijose esantiems privatiems DC, atkūrimo (įskaitant siektiną atkūrimo terminą, atkūrimo momentą ir atkūrimo kriterijus, kuriais vadovaujantis galima nustatyti, kada kritinių VII veikla sėkmingai atkurta) karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitų krizių atvejais;

34.3. informaciją apie kritinių VII kopijos parengimui ir perdavimui Nesiribojančių valstybių teritorijose esantiems privatiems DC bei kritinių VII veiklos iš kritinių VII kopijos atkūrimui taikytinus asmens duomenų apsaugos, kibernetinio saugumo reikalavimus;

34.4. asmenų, atsakingų už veiksmų koordinavimą atkuriant kritinių VII veiklą, kontaktinę informaciją (vardas, pavardė, mobiliojo ryšio telefono numeris, elektroninio pašto adresas). Pasikeitus šiems asmenims, ši kontaktinė informacija turi būti atnaujinta ne vėliau kaip per vieną darbo dieną nuo jos pasikeitimo dienos.

35. Kritinių VII valdytojas arba jo pavedimu kritinių VII tvarkytojas privalo parengti ar atnaujinti kibernetinio saugumo politiką įgyvendinančius dokumentus ar kitus VII veiklos tęstinumo užtikrinimą reglamentuojančius dokumentus dėl pasirengimo karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitiems krizių atvejams ir juose nurodyti:

35.1. darbo procedūras, kurias atliks tol, kol bus atkurta kritinių VII veikla;

35.2. kritinių VII veiklos iš kritinių VII kopijos, laikomos Nesiribojančių valstybių teritorijose esančiuose privačiuose DC, atkūrimo procedūras;

35.3. kritinių VII veiklos iš kritinių VII kopijos, laikomos Nesiribojančių valstybių teritorijose esančiuose privačiuose DC, atkūrimo patikimumo patikrinimo instrukcijas ir pateikti informaciją apie siektiną kritinių VII veiklos atkūrimo laiką, atkūrimo momentą ir atkūrimo kriterijus, kuriais vadovaujantis galima nustatyti, kada kritinių VII veikla laikoma atkurta;

35.4. kritinių VII administratorių slaptažodžių saugojimo, keitimo ir panaudojimo procedūras ir instrukcijas;

35.5. kritinių VII valdytojų, kritinių VII tvarkytojų ir (ar) Valstybės skaitmeninių sprendimų agentūros atstovų tapatybės nustatymo ir prieigos prie kritinių VII valdymo procedūras ir instrukcijas;

35.6. taikytinas asmens duomenų apsaugos, kibernetinio saugumo kontrolės priemones tol, kol bus atkurta kritinių VII veikla;

35.7. už kritinių VII veiklos atkūrimą atsakingą asmenį ar asmenis, kurie karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais būtų atsakingi už kritinių VII veiklos atkūrimą ir kiekvienos kritinių VII veiklos atkūrimo procedūros atlikimą ir instrukcijos vykdymą.

36. Tuo atveju, kai kritinių VII valdytojas yra įtrauktas į Sąrašą, rengiant Aprašo 35 punkte nurodytus dokumentus turi būti suformuluotos nuostatos dėl Valstybės skaitmeninių sprendimų agentūros dalyvavimo atkuriant kritinių VII veiklą karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais. Šiame punkte nurodytu atveju Aprašo 35 punkte nurodyti dokumentai turi būti suderinti su Valstybės skaitmeninių sprendimų agentūra.

37. Aprašo 35 punkte nurodyti dokumentai turi būti parengti ar atnaujinti ne vėliau kaip per 6 mėnesius nuo Užsakymo pateikimo Valstybės skaitmeninių sprendimų agentūrai (jeigu, vadovaujantis Aprašo 14 punktu, Sutartį su Paslaugų teikėju sudaro Valstybės skaitmeninių sprendimų agentūra) arba Sutarties sudarymo dienos (jeigu, vadovaujantis Aprašo 14 punktu, Sutartį su Paslaugų teikėju sudaro kritinių VII ar kitų VII valdytojas). Šie dokumentai rengiami vadovaujantis Kibernetinio saugumo įstatymo ir jo įgyvendinamųjų teisės aktų nuostatomis.

38. Parengęs arba atnaujinęs Aprašo 35 punkte nurodytus dokumentus, kritinių VII valdytojas arba jo pavedimu tvarkytojas privalo ne vėliau kaip per 5 darbo dienas nuo jų parengimo ar atnaujinimo dienos raštu pateikti šiuos dokumentus (jei dokumentai nėra viešai skelbiami) arba nuorodas į šių dokumentų paskelbimo šaltinį (jei dokumentai viešai skelbiami) Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos, o kai, vadovaujantis Aprašo 14 punktu, Sutartį su Paslaugų teikėju sudaro Valstybės skaitmeninių sprendimų agentūra, – ir Valstybės skaitmeninių sprendimų agentūrai.

39. Kritinių VII veiklos bandomojo atkūrimo testavimo, nurodyto Aprašo 32 punkte, rezultatai fiksuojami kritinių VII veiklos atkūrimo protokoluose. Jeigu kritinių VII veiklos bandomojo atkūrimo testavimo metu nustatoma trūkumų, kritinių VII valdytojas imasi reikalingų priemonių, kad būtų užtikrinta galimybė kritinių VII veiklą atkurti iš kopijų, laikomų užsienio teritorijose esančiuose privačiuose DC.

40. Karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar kitais krizių atvejais Lietuvos Respublikos teritorijoje praradus prieigą prie kritinių VII ar sutrikus jų veiklai ir nesant galimybės atkurti kritinių VII veiklos, turi būti inicijuojamas šių kritinių VII veiklos atkūrimas iš kritinių VII kopijos, laikomos Nesiribojančių valstybių teritorijose esančiuose privačiuose DC. Šiuo atveju kritinių VII valdytojas ar jo pavedimu kritinių VII tvarkytojas apie poreikį atkurti kritinių VII veiklą iš kritinių VII kopijos praneša karo padėtį, nepaprastąją padėtį, ekstremaliąją situaciją ar krizę valdantiems subjektams, kurie priima sprendimą dėl kritinių VII veiklos atkūrimo terminų ir prioritetų, vadovaudamiesi atitinkamos situacijos valdymą reguliuojančių teisės aktų reikalavimais.

41. Kritinių VII veiklą iš kritinių VII kopijos, laikomos Nesiribojančių valstybių teritorijose esančiuose privačiuose DC, atkuria Aprašo 25 punkte nurodyti subjektai, kurie organizavo ir vykdė kritinių VII kopijos parengimą ir perdavimą Nesiribojančių valstybių teritorijose esantiems privatiems DC, kritinių VII veiklos tęstinumo valdymo planuose nustatytais terminais ir sąlygomis.

42. Karo padėties, nepaprastosios padėties, ekstremaliųjų situacijų ar krizių atvejais Lietuvos Respublikos teritorijoje praradus prieigą prie kritinių VII ar sutrikus jų veiklai, už kritinių VII veiklos atkūrimą atsakingi asmenys pagal kompetenciją imasi veiksmų, aprašytų

Valstybės mobilizacijos plane ir (ar) Civilinės mobilizacijos institucijos mobilizacijos planuose, siekdami, kad, vadovaujantis karo padėtį, nepaprastąją padėtį, ekstremaliąją situaciją ar krizę valdančių subjektų sprendimu, kritinių VII veikla būtų atkurta Lietuvos Respublikos teritorijoje ar už jos ribų.

43. Praradus prieigą prie kitų VII ar sutrikus jų veiklai ir nesant galimybės jos atkurti, turi būti inicijuojamas šių VII veiklos atkūrimas iš jų kopijos, laikomos VDC.

44. Kitų VII veiklą iš kopijos, laikomos VDC, atkuria Aprašo 25 punkte nurodyti subjektai, kurie organizavo ir vykdė kitų VII kopijos parengimą ir perdavimą VDC, kitų VII veiklos tęstinumo valdymo planuose nustatytais terminais ir sąlygomis.

_____