LIETUVOS VYRIAUSIASIS ARCHYVARAS

ĮSAKYMAS

DĖL LIETUVOS VYRIAUSIOJO ARCHYVARO TARNYBOS IR VALSTYBĖS ARCHYVŲ KIBERNETINIO SAUGUMO VALDYMO DOKUMENTŲ PATVIRTINIMO

Nr.
Vilnius

Vadovaudamasi Lietuvos Respublikos kibernetinio saugumo įstatymo 14 straipsnio 1 dalies 1 punktu ir 2 dalimi bei įgyvendindama Kibernetinio saugumo reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo":

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

1.1. Tinklų ir informacinių sistemų kibernetinio saugumo politiką;

1.2. Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarkos aprašą;

1.3. Kibernetinių incidentų valdymo planą;

1.4. Žurnalinių įrašų valdymo tvarkos aprašą;

1.5. Tinklų ir informacinių sistemų veiklos tęstinumo valdymo tvarkos aprašą;

1.6. Atsarginių duomenų kopijų valdymo tvarkos aprašą;

1.7. Tiekimo grandinės saugumo valdymo tvarkos aprašą;

1.8. Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, tvarkos aprašą;

1.9. Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarkos aprašą;

1.10. Kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarkos aprašą;

1.11. Kriptografijos ir šifravimo naudojimo tvarkos aprašą;

1.12. Fizinės apsaugos tvarkos aprašą;

1.13. Turto valdymo tvarkos aprašą

1.14. Prieigų valdymo tvarkos aprašą.

2. P a v e d u valstybės archyvų direktoriams supažindinti su šiuo įsakymu visus valstybės archyvų darbuotojus.

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

3.1. Lietuvos vyriausiojo archyvaro 2015 m. liepos 1 d. įsakymą Nr. (1.3 E)VE-45 „Dėl Elektroninio archyvo informacinės sistemos duomenų saugos nuostatų patvirtinimo" su visais pakeitimais ir papildymais;

3.2. Lietuvos vyriausiojo archyvaro 2016 m. balandžio 11 d. įsakymą Nr. (1.3 E)VE-44 „Dėl Elektroninio archyvo informacinės sistemos saugaus elektroninės informacijos tvarkymo taisyklių, Elektroninio archyvo informacinės sistemos naudotojų administravimo

taisyklių ir Elektroninio archyvo informacinės sistemos veiklos tęstinumo valdymo plano patvirtinimo“ su visais pakeitimais ir papildymais;

3.3. Lietuvos vyriausiojo archyvaro 2022 m. gegužės 12 d. įsakymą Nr. VE-24 „Dėl kibernetinių incidentų valdymo tvarkos aprašo patvirtinimo" su visais pakeitimais ir papildymais.

4. N u s t a t a u, kad šis įsakymas įsigalioja 2026 m. balandžio 17 d.

Lietuvos vyriausioji archyvarė Inga Zakšauskienė

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų kibernetinio saugumo politikos dokumentas (toliau – Kibernetinio saugumo politikos dokumentas) yra pagrindinis Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) kibernetinio saugumo valdymo dokumentas, kuris apibrėžia kibernetinio saugumo tikslus, teisės aktus, atsakingų asmenų funkcijas ir atsakomybes, įsipareigojimus darbuotojams ir trečiosioms šalims.

2. Valstybinę archyvų sistemą sudaro LVAT ir valstybės archyvai:

2.1. Lietuvos valstybės istorijos archyvas;

2.2. Lietuvos valstybės naujasis archyvas;

2.3. Lietuvos centrinis valstybės archyvas;

2.4. Lietuvos ypatingasis archyvas;

2.5. Lietuvos literatūros ir meno archyvas;

2.6. Vilniaus regioninis valstybės archyvas;

2.7. Kauno regioninis valstybės archyvas;

2.8. Klaipėdos regioninis valstybės archyvas;

2.9. Šiaulių regioninis valstybės archyvas.

3. Kibernetinio saugumo politikos dokumento tikslas – užtikrinti kibernetinį saugumą, kuris apima tris pagrindinius aspektus:

3.1. konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo;

3.2. vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo;

3.3. prieinamumą – užtikrinimą, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti valstybinės archyvų sistemos įstaigų veiklą.

4. Valstybinės archyvų sistemos įstaigų kibernetinis saugumas grindžiamas kibernetinio saugumo principais, numatytais Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

5. Kibernetinio saugumo politikos dokumente vartojamos sąvokos:

5.1. **Atitikties vertinimas** – valstybinės archyvų sistemos įstaigų atitikties vertinimas reikalavimams, nustatytiems Kibernetinio saugumo įstatyme, Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Nutarimas Nr. 818), šiame Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei standartuose;

5.2. **Kibernetinio saugumo vadovas** – asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

5.3. **Rizikos vertinimas** – rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą pagal Lietuvos vyriausiajam archyvarui patvirtintą Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarkos aprašą;

5.4.**Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

6. Kitos šiame Kibernetinio saugumo politikos dokumente vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Kibernetinio saugumo įstatyme.

II SKYRIUS
TEISĖS AKTAI

7. Kibernetinį saugumą reglamentuojančių teisės aktų ir standartų, kuriais vadovaujasi valstybinės archyvų sistemos įstaigos, sąrašas:

7.1. Kibernetinio saugumo įstatymas;

7.2. Lietuvos Respublikos komercinių paslapčių teisinės apsaugos įstatymas;

7.3. Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

7.4. Lietuvos Respublikos konkurencijos įstatymas;

7.5. Lietuvos Respublikos viešųjų pirkimų įstatymas;

7.6. Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas;

7.7. Nutarimas Nr. 818;

7.8. Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymas Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo";

7.9. Lietuvos Respublikos dokumentų ir archyvų įstatymas;

7.10. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

7.11. Lietuvos standartas LST ISO/IEC ISO 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai";

7.12. Lietuvos standartas LST ISO/IEC 27002:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės";

7.13. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (OL 2016 L 119, p. 1) (toliau – Reglamentas (ES) 2016/679);

7.14. 2014 m. liepos 23 d. Europos Parlamento ir Tarybos reglamentas (ES) Nr. 910/2014 dėl elektroninės atpažinties ir elektroninių operacijų patikimumo užtikrinimo paslaugų vidaus rinkoje, kuriuo panaikinama Direktyva 1999/93/EB;

7.15. kitais teisės aktais, reglamentuojančiais kibernetinį saugumą.

8. Sudarytas kibernetinio saugumo įgyvendinimą reglamentuojančių dokumentų sąrašas (žr. 2 priedas).

III SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

9. Valstybinės archyvų sistemos įstaigos privalo užtikrinti žmogiškųjų ir finansinių išteklių skyrimą kibernetinio saugumo valdymui.

10. Lietuvos vyriausiasis archyvaras ar jo įgaliotas asmuo įsakymu paskiria:

10.1. Kibernetinio saugumo vadovą. LVAT privalo Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos (toliau – NKSC) Kibernetinio saugumo informacinėje sistemoje (toliau – KSIS) pateikti kibernetinio saugumo vadovo kontaktinę informaciją ir informuoti apie paskirtą kibernetinio saugumo vadovą valstybinės archyvų sistemos įstaigos darbuotojus. LVAT gali iš tiekėjo įsigyti paslaugas, kurias teikiant būtų atliekamos kibernetinio saugumo vadovo ir (ar) saugos įgaliotinio funkcijos;

10.2. Saugumo operacijų centrą (toliau – SOC). SOC funkcijas gali vykdyti ir kiti valstybinės archyvų sistemos įstaigų asmenys ir (ar) paslaugų teikėjai. LVAT gali iš tiekėjo įsigyti paslaugas, kurias teikiant būtų atliekamos SOC funkcijos;

10.3. Veiklos tęstinumo valdymo grupę ir veiklos atkūrimo grupę;

11. Valstybinės archyvų sistemos įstaigų vadovai ar jų įgalioti asmenys įsakymu paskiria:

11.1. TIS savininką;

11.2. TIS administratorių;

11.3. Fizinės apsaugos įgaliotinį.

12. Kibernetinio saugumo vadovas, koordinuodamas ir prižiūrėdamas Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų įgyvendinimą, turi atlikti šias funkcijas:

12.1. užtikrinti, kad būtų parengtas ir periodiškai atnaujinamas Kibernetinio saugumo politikos dokumentas ir kibernetinio saugumo įgyvendinimą reglamentuojantys dokumentai ir kad TIS įgyvendintų šiuose dokumentuose nustatytus reikalavimus;

12.2. organizuoti valstybinės archyvų sistemos įstaigų atitikties vertinimą, rengti ir teikti tvirtinti Lietuvos vyriausiajam archyvarui ar jo įgaliotam asmeniui Atitikties vertinimo ataskaitą ir Neatitikčių šalinimo planą bei privalomą informaciją apie juos ne vėliau kaip per 5 darbo dienas pateikti į NKSC administruojamą KSIS;

12.3. organizuoti rizikos vertinimą ir dalyvauti rizikos vertinimo procese, rengti ir teikti tvirtinti Lietuvos vyriausiajam archyvarui ar jo įgaliotam asmeniui Rizikos vertinimo ataskaitas ir rizikos valdymo planus bei privalomą informaciją apie juos ne vėliau kaip per 5 darbo dienas pateikti į NKSC administruojamą KSIS;

12.4. organizuoti TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymą, rengti ir teikti tvirtinti Lietuvos vyriausiajam archyvarui ar jo įgaliotam asmeniui TIS veiklos tęstinumo valdymo plano veiksmingumo išbandymo rezultatų ataskaitas bei privalomą informaciją apie juos ne vėliau kaip per 5 darbo dienas pateikti į NKSC administruojamą KSIS;

12.5. organizuoti valstybinės archyvų sistemos įstaigos darbuotojų kibernetinės saugos mokymus ir užtikrinti darbuotojų informuotumą apie grėsmes ir prevencines priemones;

12.6. organizuoti kibernetinės saugos priemonių diegimą ir vykdyti jų priežiūrą bei stebėseną;

12.7. valdyti TIS kibernetinius incidentus ir bendradarbiauti su kompetentingomis institucijoms, tiriančiomis kibernetinius incidentus bei neteisėtas veikas, susijusias su kibernetiniais incidentais;

12.8. teikti TIS administratoriui, naudotojams ir kitiems atsakingiems asmenims privalomus vykdyti nurodymus ir pavedimus, susijusius su Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų įgyvendinimu;

12.9. atlikti kitas Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

13. Kibernetinio saugumo vadovas negali vykdyti funkcijų, susijusių su TIS administravimu ar kitomis pareigybėmis, susijusiomis su techninės kompiuterinės įrangos ar programinės įrangos priežiūra ir valdymu.

14. TIS savininko funkcijos:

14.1. kurti ir įgyvendinti TIS strategiją;

14.2. planuoti TIS veiklas ir teikti privalomus nurodymus TIS administratoriui;

14.3. užtikrinti tinkamą TIS veikimą ir saugumą bei skatinti jų našumą;

14.4. užtikrinti tinkamą TIS problemų valdymą;

14.5. planuoti, vykdyti ir prižiūrėti TIS projektus;

14.6. ieškoti ir diegti naujus TIS sprendimus efektyvumui didinti;

14.7. atlikti kitas Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir jam priskirtas funkcijas.

15. TIS administratoriaus funkcijos:

15.1. valdyti TIS naudotojų prieigos teises;

15.2. prižiūrėti TIS komponentus (kompiuterių, operacinių sistemų, duomenų bazių, taikomųjų programų, saugasienių, įsibrovimo aptikimo sistemų);

15.3. valdyti TIS komponentų sąranką;

15.4. nustatyti TIS pažeidžiamas vietas;

15.5. nustatyti ir stebėti saugumo reikalavimų atitiktį, reagavimą į kibernetinius incidentus;

15.6. vykdyti TIS komponentų, įskaitant kibernetinio saugumo priemones, diegimą / išdiegimą.

16. Fizinės apsaugos įgaliotinio funkcijos nustatytos Fizinės apsaugos tvarkos apraše.

17. SOC funkcijos nustatytos Kibernetinių incidentų valdymo plane.

18. Veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės funkcijos nustatytos Veiklos tęstinumo valdymo tvarkos apraše.

IV SKYRIUS
ĮSIPAREIGOJIMAI

19. Kibernetinio saugumo politikos dokumente ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų privalo laikytis visi valstybinės archyvų sistemos įstaigų darbuotojai ir trečiosios šalys.

20. Darbuotojai su Kibernetinio saugumo politika ir kibernetinio saugumo įgyvendinimą reglamentuojančiais dokumentais yra supažindinami Dokumentų valdymo sistemos priemonėmis . Už supažindinimą su Kibernetinio saugumo politika ir kibernetinio saugumo įgyvendinimą reglamentuojančiais dokumentais bei jų pakeitimais yra atsakingas Kibernetinio saugumo vadovas.

21. Valstybinės archyvų sistemos įstaigos, vadovaudamosi Nutarimu Nr. 818, siekdamos mažinti galinčias kilti rizikas TIS paslaugų, darbų ar įrangos pirkimams, susijusiems su TIS projektavimu, kūrimu, diegimu, naudojimu, priežiūra, modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, trečiosioms šalims (įskaitant subtiekėjus) nustato reikalavimus pagal Tiekimo grandinės saugumo valdymo tvarkos aprašą ir juos numato sutartyse su trečiųjų šalių paslaugų teikėjais (įskaitant subtiekėjus).

22. Valstybinės archyvų sistemos įstaigos sudaro trečiųjų šalių paslaugų teikėjų sąrašą (įskaitant subtiekėjus), jį tvarko ir ne rečiau kaip kartą per metus peržiūri ir atnaujina pasikeitus sutartims arba įvykus reikšmingiems pokyčiams ar reikšmingiems incidentams, susijusiems su trečiųjų šalių paslaugų teikėjais (įskaitant subtiekėjus).

23. NKSC, atlikdamas valstybinės archyvų sistemos įstaigos patikrinimą, turi teisę pareikalauti, o valstybinės archyvų sistemos įstaiga privalo per 5 darbo dienas nuo NKSC prašymo gavimo dienos, pateikti:

23.1. Kibernetinio saugumo politikos dokumento ir kibernetinio saugumo įgyvendinimą reglamentuojančių dokumentų kopijas;

23.2. Atliktų kibernetinio saugumo auditų, atitikties vertinimo ataskaitos ir nustatytų neatitikčių šalinimo plano, rizikų vertinimo ataskaitos ir rizikos valdymo planų kopijas;

23.3. Veiklos tęstinumo valdymo plano išbandymo ataskaitos kopiją.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

24. Kibernetinio saugumo politikos dokumentas ne rečiau kaip kartą per metus arba pasikeitus reikšmingoms aplinkybėms turi būti peržiūrimas, prireikus atnaujinamas ir iš naujo patvirtinamas pagal šio Aprašo 1 priede nustatytą apskaitos žurnalo formą.

_____

Tinklų ir informacinių sistemų kibernetinio saugumo politikos
1 priedas

(Apskaitos žurnalo forma)

TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKOS DOKUMENTO PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	Statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Tinklų ir informacinių sistemų kibernetinio saugumo politikos
2 priedas

KIBERNETINIO SAUGUMO POLITIKOS ĮGYVENDINIMĄ REGLAMENTUOJANČIŲ DOKUMENTŲ SĄRAŠAS

1. Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarkos aprašas;
2. Kibernetinių incidentų valdymo planas;
3. Žurnalinių įrašų valdymo tvarkos aprašas;
4. Tinklų ir informacinių sistemų veiklos tęstinumo valdymo tvarkos aprašas;
5. Atsarginių duomenų kopijų valdymo tvarkos aprašas;
6. Tiekimo grandinės saugumo valdymo tvarkos aprašas;
7. Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, tvarkos aprašas;
8. Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarkos aprašas;
9. Kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarkos aprašas;
10. Kriptografijos ir šifravimo naudojimo tvarkos aprašas;
11. Fizinės apsaugos tvarkos aprašas;
12. Turto valdymo tvarkos aprašas;
13. Prieigų valdymo tvarkos aprašas.

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

TINKLŲ IR INFORMACINIŲ SISTEMŲ RIZIKOS VERTINIMO IR VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) tinklų ir informacinių sistemų (toliau – TIS) kibernetinio saugumo rizikos vertinimo ir valdymo procesą, už šį procesą atsakingų padalinių ir darbuotojų funkcijas ir atsakomybes.

2. Aprašas taikomas atliekant valstybinės archyvų sistemos įstaigų TIS kibernetinio saugumo rizikos vertinimą.

3. Šiame Apraše naudojamos sąvokos:

3.1. **Kibernetinio saugumo rizika** (toliau – rizika) – potencialus praradimas arba sutrikimas, kurį gali sukelti kibernetinis incidentas. Kibernetinio saugumo rizika išreiškiama kaip tokio praradimo arba sutrikimo masto ir kibernetinio incidento tikimybės derinys;

3.2. **Likutinė rizika** – rizika, liekanti po rizikos valdymo priemonių įgyvendinimo;

3.3. **Rizikų registras** – šio Aprašo 2 priede esančios Rizikos registro formos pagrindu parengtas valstybinės archyvų sistemos įstaigos identifikuotų rizikų ir jų savininkų sąrašas, taip pat rizikos vertinimo rezultatai;

3.4. **Rizikos savininkas** – valstybinės archyvų sistemos įstaigos darbuotojas, Rizikų registre paskirtas vykdyti rizikos savininko funkcijas, t. y. vertinti ir stebėti riziką bei užtikrinti jos efektyvų valdymą;

3.5. **Rizikos valdymo priemonės vykdytojas** – valstybinės archyvų sistemos įstaigos darbuotojas, Rizikų valdymo plane paskirtas vykdyti rizikos valdymo priemonės vykdytojo funkcijas, t. y., įgyvendinti rizikos valdymo priemonę nepriimtinai rizikai valdyti;

3.6. **Rizikos vertinimas** – šiame Apraše aprašytas rizikos vertinimo procesas, apimantis rizikų identifikavimą, jų analizę ir įvertinimą;

3.7. **Rizikos vertinimo ataskaita** (toliau – RVA) – Lietuvos vyriausiojo archyvaro patvirtintas dokumentas, kuriame aprašomi rizikos vertinimo rezultatai, įskaitant, tačiau neapsiribojant, rizikos vertinimo metu nustatytais apibendrintais rezultatais: identifikuotomis grėsmėmis, spragoms ir rizikomis, jų tikimybe ir poveikiu veiklai, rizikos lygiais ir rizikos valdymo priemonėmis;

3.8. **Rizikų valdymo planas** (toliau – RVP) – Rizikos valdymo plano formos pagrindu parengtas ir Lietuvos vyriausiojo archyvaro patvirtintas valstybinės archyvų sistemos įstaigos nepriimtinų rizikų valdymo priemonių, jų įgyvendinimo terminų, reikalingų išteklių bei rizikos valdymo priemonių vykdytojų planas;

4. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Lietuvos Respublikos kibernetinio saugumo įstatyme.

5. Aprašas yra skirtas visiems valstybinės archyvų sistemos įstaigos darbuotojams, dalyvaujantiems rizikos vertinimo procese. Šio Aprašo nuostatos taip pat gali būti taikomos valstybinės archyvų sistemos įstaigos tiekėjams (įskaitant subtiekėjus), kiek tai susiję su teikiamomis paslaugomis ir numatytais kibernetinio saugumo reikalavimais pagal Kibernetinio saugumo reikalavimų aprašą, patvirtintą Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo".

II SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

6. Lietuvos vyriausiojo archyvaro funkcijos ir atsakomybės:

6.1. tvirtina RVA ir RVP;

6.2. atsako už tinkamą informacijos saugumo rizikos vertinimą.

7. Valstybinės archyvų vadovų funkcijos ir atsakomybės:

7.1. atsako už tinkamą informacijos saugumo rizikos vertinimą ir valdymą;

7.2. skiria žmogiškuosius išteklius rizikos vertinimui;

7.3. skiria reikiamus išteklius RVP numatytoms priemonėms įgyvendinti.

8. Kibernetinio saugumo vadovo funkcijos ir atsakomybės:

8.1. koordinuoja ir kontroliuoja rizikos vertinimo ir valdymo procesą;

8.2. teikia derinti ir tvirtinti RVA ir RVP;

8.3. kartu su valstybinės archyvų sistemos įstaigos TIS savininkais identifikuoja ir klasifikuoja TIS;

8.4. teikia siūlymą įstaigos vadovui dėl darbuotojo paskyrimo konkrečios rizikos savininku;

8.5. kartu su TIS ir rizikų savininkais identifikuoja esamas ir galimas TIS grėsmes ir saugumo spragas bei iš to galinčias kilti rizikas;

8.6. identifikuotas rizikas registruoja Rizikų registre;

8.7. kartu su rizikos savininkais kiekvienai rizikai nustato rizikos lygį (įvertina rizikos poveikio ir tikimybės lygį) ir padeda priimti sprendimą dėl rizikos priimtinumo ar nepriimtinumo;

8.8. padeda rizikos savininkams parinkti ir RVP suplanuoti rizikos valdymo priemones nepriimtinoms rizikoms valdyti;

8.9. padeda rizikos valdymo priemonių vykdytojams įgyvendinti jiems paskirtas priemones;

8.10. konsultuoja darbuotojus rizikos vertinimo ir valdymo klausimais;

8.11. Kibernetinio saugumo įstatymo ir jo įgyvendinimą reglamentuojančių teisės aktų nustatyta tvarka ir terminais į Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) administruojamą Kibernetinio saugumo informacinę sistemą (toliau – KSIS) pateikia informaciją apie valstybinės archyvų sistemos įstaigos atliktą Rizikos vertinimą.

9. Rizikos savininko funkcijos ir atsakomybės:

9.1. kartu su TIS savininkais vertina esamas ir galimas TIS grėsmes bei spragas,

kurių sąsaja sukelia riziką;

9.2. nustato rizikos lygį (įvertina rizikos poveikio ir tikimybės lygį) ir priima sprendimą dėl rizikos priimtinumo ar nepriimtinumo;

9.3. nustato rizikos valdymo būdą;

9.4. parenka ir RVP suplanuoja rizikos valdymo priemones nepriimtinoms rizikoms valdyti, suderinęs su įstaigos vadovu paskiria už šių priemonių įgyvendinimą atsakingus vykdytojus ir nustato rizikos valdymo priemonių įgyvendinimo terminus;

9.5. įvertina likutinės rizikos lygį;

9.6. stebi rizikos valdymo priemonių įgyvendinimą ir efektyvumą;

9.7. vykdo nustatytos rizikos stebėseną;

9.8. stebi rizikos valdymo pokyčius ir vertina, ar RVP numatytos rizikos valdymo priemonės vis dar yra veiksmingos;

9.9. kiekvieną ketvirtį teikia rizikos valdymo pokyčių situaciją kibernetinio saugumo vadovui.

10. TIS savininko funkcijos ir atsakomybės:

10.1. padeda rizikos savininkams identifikuoti ir įvertinti kibernetinio saugumo rizikas, galinčias pasireikšti TIS, už kurių valdymą jis yra atsakingas;

10.2. padeda rizikos savininkams RVP suplanuoti ir parinkti rizikos valdymo priemones nepriimtinoms rizikoms valdyti.

III SKYRIUS
RIZIKOS VERTINIMAS

11. Kibernetinio saugumo vadovas ne rečiau kaip kartą per metus organizuoja valstybinės archyvų sistemos įstaigos rizikos vertinimą.

12. Prireikus gali būti organizuojamas neeilinis rizikos vertinimas. Neeilinis rizikos vertinimas gali būti atliekamas įvykus esminių pokyčių, galinčių daryti įtaką valstybinės archyvų sistemos įstaigos veiklai ir kibernetiniam saugumui arba įvykus dideliam kibernetiniam incidentui.

13. Rizikos vertinimo procesą sudaro trys pagrindiniai etapai: rizikos identifikavimas; rizikos analizė; rizikos įvertinimas.

14. Rizikos identifikavimo etapas.

14.1. Kibernetinio saugumo vadovas kartu su įstaigos TIS savininkais identifikuoja ir suklasifikuoja TIS, kurių atžvilgiu atliekamas rizikos vertinimas;

14.2. Kibernetinio saugumo vadovas identifikuoja visas galimas grėsmes, kurios gali kelti pavojų identifikuotoms TIS, sudarydamas grėsmių sąrašą. Grėsme laikomas bet koks išorinis ar vidinis veiksnys, galintis išnaudoti sistemos spragą – programišių ataka, elektros dingimas, darbuotojo klaida ir kt.

Grėsmės gali būti identifikuojamos šiais būdais:

14.2.1. renkant informaciją iš vidinių šaltinių (TIS audito žurnalai);

14.2.2. gaunant informaciją iš išorinių šaltinių (atviruųjų šaltinių žvalgybos priemonių, komercinės grėsmių žvalgybos pranešimų ir kt.);

14.2.3. atliekant kibernetinio saugumo valdymo atitikties Kibernetinio saugumo įstatymo ir jo įgyvendinimą reglamentuojančių teisės aktų bei Kibernetinio saugumo politikos ir jos įgyvendinimą reglamentuojančių vidaus teisės aktų reikalavimams vertinimą;

14.2.4. analizuojant kibernetinio saugumo incidentų ataskaitas.

14.3. Įvertinamos valstybinės archyvų sistemos įstaigoje egzistuojančios spragos ir parenkamos aktualios grėsmės, keliančios riziką turtui. Spraga laikoma sistemos ar proceso silpnoji vieta – neatnaujinta programinė įranga, neužrakintos durys ir kt.

Spragos gali būti nustatomos šiais būdais:

14.3.1. atliekant automatizuotus TIS skenavimus;

14.3.2. atliekant TIS saugumo testavimus ir įvertinimus;

14.3.3. atliekant TIS įsilaužimų testavimus;

14.3.4. apklausiant darbuotojus;

14.3.5. atliekant fizinę apžiūrą;

14.3.6. atliekant kibernetinio saugumo valdymo atitikties Kibernetinio saugumo įstatymo ir jo įgyvendinimą reglamentuojančių teisės aktų bei Kibernetinio saugumo politikos ir jos įgyvendinimą reglamentuojančių vidaus teisės aktų reikalavimams vertinimą;

14.3.7. atliekant kibernetinio saugumo auditus;

14.3.8. analizuojant dokumentus.

14.4. Spragos gali būti nustatytos šiose srityse:

14.4.1. veiklos procesuose ir procedūrose;

14.4.2. žmogiškuosiuose ištekliuose;

14.4.3. fizinėje aplinkoje;

14.4.4. TIS sąrankoje (konfigūracijoje);

14.4.5. techninėje ir programinėje įrangoje;

14.4.6. trečiųjų šalių teikiamose paslaugose.

14.5. Kibernetinio saugumo vadovas visas identifikuotas rizikas registruoja Rizikų registre, kiekvienai jų kartu įstaigos vadovu priskirdamas ir rizikos savininką.

14.6. Rizikos identifikavimo metu surenkama ir informacija apie įstaigos turimas rizikos valdymo priemones, įskaitant kibernetinio saugumo priemones.

15. Rizikos analizės etapas:

15.1. Rizikos analizės metu kibernetinio saugumo vadovas kartu su rizikos ir TIS savininkais įvertina kiekvienos rizikos tikimybę ir poveikį balais nuo 1 iki 5 balų, vadovaudamasis Aprašo 5 priede pateiktais tikimybių ir poveikio vertinimo kriterijais;

15.2. Įvertinus poveikį ir tikimybę, vadovaujantis Rizikos vertinimo lentele (Aprašo 4 priedas) apskaičiuojamas rizikos lygis nuo 1 iki 25 balų. Rizikos lygis nustatomas padauginus rizikos tikimybės ir poveikio vertinimo balus;

15.3. Siekiant nustatyti rizikos tikimybę ir poveikį, gali būti atliekamas įstaigos turimų rizikos valdymo priemonių, įskaitant kibernetinio saugumo priemones, vertinimas.

16. Rizikos vertinimo etapas:

16.1. Kibernetinio saugumo vadovas kartu su rizikos savininkais priima sprendimą dėl rizikos priimtinumo ar nepriimtinumo;

16.2. Rizika laikoma priimtina, jei jos balas neviršija 10;

16.3. Rizika, įvertinta balais nuo 11 iki 25, laikoma nepriimtina;

16.4. Esant poreikiui, mažesnį nei 10 balą turinti rizika taip pat gali būti įvertinama kaip nepriimtina (pvz., jei kyla rizika įstaigos kritinei TIS ir pan.);

16.5. TIS savininkai nustatytoms nepriimtinoms rizikoms valdyti parenka vieną iš rizikos valdymo būdų:

16.5.1. mažinti riziką – taikyti tinkamas rizikos valdymo priemones, siekiant sumažinti riziką;

16.5.2. prisiimti riziką – sąmoningai prisiimti riziką, užtikrinant, jog ji aiškiai atitinka įstaigos strateginius tikslus ir rizikos prisiėmimo kriterijus. Neretai rizika prisiimama tais atvejais, kai rizikos valdymo (mažinimo) priemonės kaštai akivaizdžiai viršija galimus finansinius ar reputacinius nuostolius incidento atveju;

16.5.3. vengti rizikos – užkirsti kelią veiksmams, dėl kurių galėtų kilti rizika, arba atsisakyti veiksmų, dėl kurių kyla rizika;

16.5.4. perduoti riziką – perduoti riziką kitoms šalims, pavyzdžiui, draudimo įmonėms ar trečiųjų šalių paslaugų teikėjams.

16.6. Jei nepriimtinai rizikai valdyti parenkamas valdymo būdas „mažinti riziką“ arba „perduoti riziką“, RVP tam turi būti numatyta konkreti priemonė arba priemonės.

16.7. Nepriimtinoms rizikoms valdyti rizikos savininkai parengia RVP, kuriame nurodo nepriimtinų rizikų valdymo priemones, jų įgyvendinimo prioritetus ir terminus bei reikiamus išteklius, taip pat paskiria rizikos valdymo priemonės vykdytojus. Nepriimtinoms rizikoms valdyti RVP numačius rizikos valdymo priemones, rizikų savininkai turi įvertinti, koks bus kiekvienos rizikos likutinės rizikos lygis (tikimybės ir poveikio lygio vertė), įgyvendinus visas priemonių plane numatytas priemones, ir nutarti, ar tokia likutinė rizika yra priimtina.

17. Atlikęs rizikos vertinimą kibernetinio saugumo vadovas parengia ir teikia valstybės archyvų vadovams derinti, o Lietuvos vyriausiam archyvarui tvirtinti RVA, kurioje pateikia TIS, kurių atžvilgiu atliktas rizikos vertinimas, sąrašą, nurodydamas identifikuotas grėsmes ir spragas, rizikų sąrašą, rizikų tikimybės ir poveikio vertinimo rezultatus, spragų vertinimo bei rizikos lygio apskaičiavimo rezultatus. Ir RVA, ir prie jos pridedamas RVP registruojami įstaigos dokumentų valdymo sistemoje.

18. Kibernetinio saugumo vadovas ne vėliau kaip per 5 darbo dienas nuo RVA ir RVP patvirtinimo dienos į KSIS pateikia apibendrintus duomenis, nurodydamas identifikuotas rizikas, jų tikimybę ir poveikį veiklai, rizikos lygius ir valdymo priemones.

19. RVA ir RVP saugomi ne mažiau kaip 3 metus.

20. NKSC, atlikdamas valstybinės archyvų sistemos įstaigos patikrinimą, turi teisę pareikalauti jos pateikti RVA ir RVP kopijas. Kibernetinio saugumo vadovas šiuos dokumentus turi pateikti į KSIS ne vėliau kaip per 5 darbo dienas nuo NKSC prašymo gavimo dienos.

IV SKYRIUS
RIZIKOS VALDYMAS IR STEBĖSENA

21. Rizikos savininkai turi nuolat stebėti rizikas ir rizikos valdymo priemonių įgyvendinimą, rizikos valdymo pokyčius, vertindami, ar RVP numatytos rizikos valdymo priemonės vis dar yra veiksmingos. Nustatę, kad rizikos valdymo priemonės neveiksmingos, rizikos savininkai RVP turi suplanuoti naujas ir (ar) papildomas priemones, siekiant sumažinti rizikas iki priimtino rizikos lygio.

22. Apie rizikos pokyčius ir RVP veiksmingumą rizikos savininkai nedelsiant turi informuoti kibernetinio saugumo vadovą.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

23. Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba atsiradus esminiams pokyčiams, galintiems turėti įtakos šiam Aprašui. Už Aprašo peržiūrą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

_____

Tinklų ir informacinių sistemų
rizikos valdymo aprašo
1 priedas

(Apskaitos žurnalo forma)

TINKLŲ IR INFORMACINIŲ SISTEMŲ RIZIKOS VERTINIMO IR VALDYMO TVARKOS APRAŠO PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	Statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Tinklų ir informacinių sistemų rizikos valdymo aprašo
2 priedas

(Rizikų registro forma)

RIZIKŲ REGISTRAS

Eil. Nr.	TIS ar TIS grupės pavadinimas	Grėsmė	Spraga	Rizikos poveikis	Rizikos tikimybė	Rizikos lygis	Priimtinumas	Rizikos savininkas	Rizikos valdymo būdas	Rizikos valdymo priemonės pavadinimas ir aprašymas	Likutinės rizikos tikimybė	Likutinės rizikos poveikis	Likutinės rizikos lygis
	(1)	*(2)*	*(3)*	*(4)*	*(5)*	*(6)*	*(7)*	*(8)*	*(9)*	*(10)*	*(11)*	*(12)*	*(13)*
1.													

Pildymo instrukcija:
(1) Nurodomas TIS ar grupės pavadinimas (pvz.: Personalo valdymo informacinė sistema; vidinio tinklo įranga, esanti patalpose, adresu [Patalpų adresas] ir pan.);
(2) Nurodomos su TIS susijusios grėsmės (pvz.: potvynis, socialinė inžinerija, paslaugų teikimo sutrikdymas, gaisras ir pan.);
(3) Nurodomos su TIS susijusios spragos (pvz.: patalpos, kuriose saugoma tinklo įranga, nėra rakinamos; jose nėra įrengtos apsaugos sistemos ir pan.);
(4) Nurodomas rizikos poveikio vertinimo balas pagal Kibernetinio saugumo rizikos vertinimo metodiką;
(5) Nurodomas rizikos tikimybės vertinimo balas pagal Kibernetinio saugumo rizikos vertinimo metodiką;
(6) Nurodomas rizikos lygio vertinimo balas pagal Kibernetinio saugumo rizikos vertinimo metodiką (tikimybės ir poveikio vertinimų balų sandauga);
(7) Nurodomas rizikos priimtinumo vertinimas, pažymint „rizika priimtina" arba „rizika nepriimtina";
(8) Nurodomos rizikos savininko pareigos, vardas ir pavardė;
(9) Nurodomas rizikos valdymo būdas pagal Kibernetinio saugumo rizikos vertinimo metodiką (mažinti riziką, prisiimti riziką, vengti rizikos arba perduoti riziką);
(10) Nurodomas rizikos valdymo priemonės, skirtos nepriimtinai rizikai mažinti, pavadinimas (gali būti pateiktas jos trumpas aprašymas);
(11) Nurodomas likutinės rizikos, kuri lieka pritaikius rizikos valdymo priemonę, tikimybės vertinimo balas pagal Kibernetinio saugumo rizikos vertinimo metodiką;
(12) Nurodomas likutinės rizikos, kuri lieka pritaikius rizikos valdymo priemonę, poveikio vertinimo balas pagal Kibernetinio saugumo rizikos vertinimo metodiką;
(13) Nurodomas likutinės rizikos, kuri lieka pritaikius rizikos valdymo priemonę, lygio vertinimo balas pagal Kibernetinio saugumo rizikos vertinimo metodiką (tikimybės ir poveikio vertinimų balų sandauga).

Tinklų ir informacinių sistemų
rizikos valdymo aprašo
3 priedas

(Rizikų valdymo plano forma)

RIZIKŲ VALDYMO PLANAS

Nr.	Priemonės pavadinimas ir aprašymas	Rizika, kuriai valdyti skirta priemonė	Prioritetas	Rizikos savininkas	Reikalingi ištekliai	Priemonės vykdytojas	Įgyvendinimo terminas

Tinklų ir informacinių sistemų
rizikos valdymo aprašo
4 priedas

TIKIMYBĖS IR POVEIKIO VERTINIMO KRITERIJAI

Tikimybės vertinimo lentelė

Tikimybė	Tikimybės kriterijus	Aprašas
Neabejotina 5 lygis	Įvykdymo paprastumas	Rizikos šaltinis neabejotinai pasieks savo tikslą, naudodamas vieną iš svarstomų puolimo būdų.
	Įvykimo tikimybė	Rizikos scenarijaus tikimybė yra ypač didelė.
	Rizikos dažnis	Rizika kyla arba gali turėti poveikį bent **kartą per mėnesį arba dažniau**.
Labai tikėtina 4 lygis	Įvykdymo paprastumas	Tikėtina, kad rizikos šaltinis savo tikslą pasieks, naudodamas vieną iš svarstomų atakos būdų.
	Įvykimo tikimybė	Rizikos scenarijaus tikimybė yra labai didelė.
	Rizikos dažnis	Rizika kyla arba gali turėti poveikį nuo **vieno karto per mėnesį iki vieno karto per pusę metų**.
Tikėtina 3 lygis	Įvykdymo paprastumas	Rizikos šaltinis gali pasiekti savo tikslą, taikydamas vieną iš svarstomų metodų puolimo būdą.
	Įvykimo tikimybė	Rizikos scenarijaus tikimybė yra didelė.
	Rizikos dažnis	Rizika kyla arba gali turėti poveikį nuo **vieno karto per pusę metų iki vieno karto per metus.**
Mažai tikėtina 2 lygis	Įvykdymo paprastumas	Rizikos šaltinis turi palyginti nedaug galimybių pasiekti savo tikslą, naudodamas vieną iš svarstomų atakos būdų.
	Įvykimo tikimybė	Rizikos scenarijaus tikimybė yra maža.
	Rizikos dažnis	Rizika kyla arba gali turėti poveikį nuo **vieno karto per metus iki vieno karto per penkerius metus**.
Netikėtina 1 lygis	Įvykdymo paprastumas	Rizikos šaltinis turi labai mažai galimybių pasiekti savo tikslą, naudodamas vieną iš svarstomų atakos būdų.
	Įvykimo tikimybė	Rizikos scenarijaus tikimybė yra labai maža.
	Rizikos dažnis	Rizika kyla arba gali turėti poveikį **vieną kartą per daugiau nei penkerius metus**.

Poveikio lygių vertinimo lentelė

Poveikis	Poveikio kriterijus	Aprašas
Katastrofini	Finansiniai	Tikėtinas nuostolis yra daugiau nei 1 500 000

s 5 lygis	nuostoliai	Eur. Nuostolis kelią grėsmę organizacijos egzistavimui, reikšmingai paveikia įmonės kapitalą, mokumą, veiklos tęstinumą.
	Veiklos tęstinumo sutrikimas	Su rizika susijęs procesas turi būti atnaujintas per ne daugiau nei 4 valandas.
	Tiekimo grandinė	Organizacija šiurkščiai pažeidžia sudarytas sutartis, partneriai nutraukia sutartis su organizacija.
	Reputacija	Nepataisoma ilgalaikė žala visuomenės pasitikėjimui organizacija ir organizacijos įvaizdžiui. Apie incidentą pranešama žiniose televizijoje, jis aptariamas laidose.
	Teisinė atitiktis	Labai didelė rizika, kad bus baudos, sankcijos, teisminiai ginčai, neatitiktis įstatymams. Valstybė gali taikyti veiklos ribojimo priemones.
	Žmogaus sveikata	Sunkūs ir / arba ilgalaikiai sužalojimai ar sveikatos sutrikimai, galima mirtis. Hospitalizacija ilgiau nei savaitė.
Kritinis 4 lygis	Finansiniai nuostoliai	Tikėtinas nuostolis yra nuo 1 500 000 iki 1 016 666 Eur.
	Veiklos tęstinumo sutrikimas	Su rizika susijęs procesas turi būti atnaujintas per 4–24 valandas.
	Tiekimo grandinė	Organizacija rimtai pažeidžia sudarytas sutartis, partneriai skiria baudas ar sankcijas organizacijai.
	Reputacija	Ilgalaikis neigiamas poveikis organizacijos įvaizdžiui. Incidentas aptariamas žiniose ir televizijoje.
	Teisinė atitiktis	Reikšminga rizika, kad bus baudos, sankcijos, teisminiai ginčai, neatitiktis įstatymams.
	Žmogaus sveikata	Galimi sužeidimai ir kelių dienų hospitalizacija.
Rimtas 3 lygis	Finansiniai nuostoliai	Tikėtinas nuostolis yra nuo 1 016 666 iki 533 333 Eur.
	Veiklos tęstinumo sutrikimas	Su rizika susijęs procesas turi būti atnaujintas per 24–48 valandas.
	Tiekimo grandinė	Organizacijos sudarytos sutartys pažeistos, pažeidimai nedideli, tačiau organizacija tikriausiai sulauks baudų iš partnerių.
	Reputacija	Laikinas neigiamas poveikis reputacijai. Incidentas minimas socialinėje medijoje ir su kibernetiniu saugumu susijusiose publikacijose.
	Teisinė atitiktis	Vidutinė rizika, kad bus baudos, sankcijos, teisminiai ginčai, neatitiktis įstatymams.
	Žmogaus sveikata	Nesunkūs sužeidimai ar sveikatos sutrikimai, hospitalizacija iki dienos trukmės.
Reikšmingas 2 lygis	Finansiniai nuostoliai	Tikėtinas nuostolis yra nuo 533 333 iki 50 000 Eur.
	Veiklos tęstinumo sutrikimas	Su rizika susijęs procesas turi būti atnaujintas per 48 valandas–7 dienas.
	Tiekimo grandinė	Organizacijos sudarytos sutartys gali būti

		pažeistos, tačiau pažeidimai minimalūs arba neturi poveikio partneriams.
	Reputacija	Trumpalaikis neigiamas poveikis organizacijos reputacijai. Incidentas minimas tarp žmonių ar socialinės medijos tinkluose.
	Teisinė atitiktis	Maža rizika, kad bus baudos, sankcijos, teisminiai ginčai, neatitiktis įstatymams.
	Žmogaus sveikata	Smulkūs bei nesunkūs sužeidimai ar sveikatos sutrikimai, hospitalizacija nereikalinga.
Mažas 1 lygis	Finansiniai nuostoliai	Tikėtinas nuostolis iki 50 000 Eur.
	Veiklos tęstinumo sutrikimas	Su rizika susijęs procesas turi būti atnaujintas per 7–30 dienų.
	Tiekimo grandinė	Nėra poveikio organizacijos sudarytoms sutartims.
	Reputacija	Nėra poveikio organizacijos reputacijai, apie incidentą nepranešama.
	Teisinė atitiktis	Nėra rizikos, kad bus baudos, sankcijos, teisminiai ginčai, neatitiktis įstatymams.
	Žmogaus sveikata	Trumpas diskomfortas arba nėra poveikio žmogaus sveikatai ar saugumui.

Tinklų ir informacinių sistemų
rizikos valdymo aprašo
5 priedas

RIZIKOS VERTINIMO LENTELĖ

Tikimybė	Poveikis				
	Mažas (1)	Reikšmingas (2)	Rimtas (3)	Kritinis (4)	Katastrofinis (5)
Neabejotina (5)	Maža	Vidutinė	Didelė	Labai didelė	Labai didelė
Labai tikėtina (4)	Maža	Vidutinė	Didelė	Didelė	Labai didelė
Tikėtina (3)	Maža	Vidutinė	Vidutinė	Didelė	Didelė
Mažai tikėtina (2)	Labai maža	Maža	Vidutinė	Vidutinė	Vidutinė
Reta (1)	Labai maža	Labai maža	Maža	Maža	Maža

Paaiškinimai

Rizikos lygis	Minimalus balas	Maksimalus balas
Labai didelė	20	25
Didelė	11	19
Vidutinė	6	10
Maža	3	5
Labai maža	1	2

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

KIBERNETINIŲ INCIDENTŲ VALDYMO PLANAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kibernetinių incidentų valdymo planas (toliau – Planas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) gebėjimą tinkamai ir laiku reaguoti į kibernetinius incidentus, sumažinti jų poveikį, atkurti pažeistus tinklus ir informacines sistemas.

2. Šiame Plane vartojamos sąvokos:

2.1. **Kibernetinis incidentas** – įvykis, dėl kurio kyla pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas (toliau – TIS), prieinamumui, autentiškumui, vientisumui arba konfidencialumui.

2.2. **Vos neįvykęs kibernetinis incidentas** – įvykis, dėl kurio galėjo būti sukeltas pavojus saugomų, perduodamų arba tvarkomų duomenų arba paslaugų, teikiamų arba prieinamų per tinklų ir informacines sistemas, prieinamumui, autentiškumui, vientisumui arba konfidencialumui, bet kuriam įvykti buvo sėkmingai užkirstas kelias arba kuris neįvyko.

2.3. **Informacinių technologijų pagalbos tarnyba (toliau – IT pagalbos tarnyba)** – valstybinės archyvų sistemos įstaigų naudojama informacinė sistema ar programinė įranga informacinių technologijų kreipiniams ir problemoms bei kibernetinio saugumo įvykiams ir incidentams, taip pat pokyčiams registruoti ir valdyti; nesant IT pagalbos tarnybos, pranešimai dėl galimo kibernetinio incidento teikiami el. paštu soc@archyvai.lt;

2.4. **Saugumo operacijų centras (toliau – SOC)** – Lietuvos vyriausiojo archyvaro ar jo įgalioto asmens paskirtas asmuo ar grupė, taip pat paslaugas teikianti trečioji šalis, atsakinga už žurnalų įrašų ir kibernetinių incidentų stebėjimą ir valdymą;

2.5. **Kibernetinio saugumo vadovas** – asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

2.6. **Kibernetinio incidento tyrimas** (toliau – Tyrimas) – techninė kibernetinio incidento analizė, kurioje nurodoma, kas, kaip, kodėl ir kada įvyko. Analizės metu būtina nustatyti pagrindinius veiksnius, dėl kurių galėjo įvykti kibernetinis incidentas.

2.7. Kitos šiame Plane vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

3. Plano privalo laikytis visi valstybinės archyvų sistemos įstaigų darbuotojai.

II SKYRIUS
KIBERNETINIO INCIDENTO VALDYMO ORGANIZAVIMAS

4. Kibernetinio incidento valdymo procese dalyvaujančių atsakingų asmenų ir institucijų sąrašas su kontaktine informacija pateikiamas šio Plano 2 priede.

5. Kibernetinio incidento valdymo metu informacija gali būti keičiamasi įvairiomis informacijos perdavimo priemonėmis, pirmenybę teikiant komunikavimui el. paštu, bendradarbiavimo platforma „TEAMS" ir telefonu. Esant poreikiui asmenys, dalyvaujantys kibernetinio incidento valdyme, gali susitikti gyvai arba organizuoti virtualų susirinkimą.

6. Kibernetinio incidento poveikis nustatomas pagal Kibernetinio incidento poveikio nustatymo kriterijus, nurodytus Plano 3 priede.

7. Jeigu kyla rizika, kad valstybinės archyvų sistemos įstaiga negalės savarankiškai suvaldyti kibernetinio incidento per maksimalų priimtiną neveikimo laiką (MTPD) (atsižvelgiant į Veiklos tęstinumo valdymo plane nustatytus konkrečių TIS neveikimo laikus), kibernetinio saugumo vadovas gali kreiptis pagalbos į Nacionalinio kibernetinio saugumo centrą prie Lietuvos Respublikos krašto apsaugos ministerijos, prieš tai suderinęs su Lietuvos vyriausiuoju archyvaru arba, jeigu incidentas kyla valstybės archyve, – su to archyvo direktoriumi ir su Lietuvos vyriausiuoju archyvaru Plano 2 priede nurodytais kontaktais.

8. Jeigu kibernetinis incidentas susijęs su asmens duomenimis ir (arba) turi nusikalstamos veikos požymių, kibernetinio saugumo vadovas koordinuoja informacijos keitimąsi su Policijos departamentu prie Lietuvos Respublikos vidaus reikalų ministerijos (toliau – Policija) ir (arba) Valstybine duomenų apsaugos inspekcija (toliau – Inspekcija), derindamas savo veiksmus su Lietuvos vyriausiuoju archyvaru, duomenų apsaugos pareigūnu ir, jei incidentas įvyko valstybės archyve, su šio archyvo direktoriumi.

9. SOC darbo režimas:

9.1. SOC funkcijas vykdo valstybinės archyvų sistemos įstaigos paskirtas asmuo ar grupė arba paslaugų teikėjas (toliau – SOC vykdytojas) ne mažiau kaip darbo dienomis 9–17 val. (9/5 režimu). Pasitelkiant išorinį paslaugų teikėją, sutartis su juo parengiama vadovaujantis Tiekimo grandinės saugumo valdymo tvarkos aprašu.

9.2. Ne darbo metu stebėseną vykdo automatizuotos priemonės, veikiančios 24/7 režimu. Aptikus kritinius įvykius, automatinis pranešimas nedelsiant siunčiamas kibernetinio saugumo vadovui ir SOC.

10. Kibernetinio incidento valdymo schema pateikta Plano 4 priede.

III SKYRIUS

INCIDENTO NUSTATYMAS IR VERTINIMAS

11. Pagrindiniai šaltiniai, kuriais naudojantis gali būti sukeltas kibernetinis incidentas ir sutrikdyta valstybinės archyvų sistemos įstaigų veikla kibernetinėje erdvėje ir (ar) paveiktos valstybinės archyvų sistemos įstaigų TIS, nurodyti Plano 5 priede.

12. Informacija apie galimą kibernetinį incidentą gali būti gauta iš įvairių informacijos šaltinių: duomenų apsaugos pareigūno, darbuotojų, TIS administratorių, SOC specialistų, automatizuotų kibernetinių įvykių ir pažeidžiamumų aptikimo priemonių, kompetentingų valstybės institucijų, kitų juridinių arba fizinių asmenų, taip pat kitų valstybių, tarptautinių organizacijų arba institucijų, atliekančių kibernetinio saugumo užtikrinimo funkcijas, ir kitų šaltinių. Informacijos pateikimo būdai – el. paštas, telefonas, socialiniai tinklai ir kitos automatizuotos priemonės.

13. Įvykus kibernetiniam incidentui arba kilus įtarimų, kad galėjo įvykti kibernetinis incidentas, valstybinės archyvų sistemos įstaigos darbuotojai turi pranešti SOC, registruodami pranešimą IT pagalbos tarnyboje, o jos nesant – elektroniniu paštu soc@archyvai.lt, ir informuoti TIS administratorių, kurio administravimo srityje įvyko incidentas (toliau – Atsakingas administratorius). Pranešime turi būti pateikta kuo išsamesnė informacija ir nurodytos visos darbuotojui žinomos aplinkybės (data, laikas, naudotojo veiksmų seka, gavimo šaltinis, spaustos nuorodos, parsisiųsti failai ir kiti kibernetinio incidento įrodymai), pvz:

- atvėrus bylą ar nuorodą, tikėtina, kenkėjiškuose el. laiškuose,
- suveikus kibernetinio saugumo priemonių apsaugoms,
- užsišifravus kompiuterio dokumentams ar informacinei sistemai,
- pastebėjus žalingą komunikaciją,
- suvedus prisijungimo duomenis galbūt apgaulingoje svetainėje,
- patyrus paslaugos atkirtimo (DoS, DDoS) atakas ar kitaip užfiksavus nepasiekiamus archyvų sistemų informacinius išteklius (svetainės, duomenų bazės, el. paštas) ilgiau nei vieną valandą,
- įtarus kad kažkas neįprasto vyksta su kompiuterine darbo vieta ar informacine sistema: sistema veikia žymiai lėčiau nei įprastai, atsiranda nežinomų failų, programų ar nuorodų, siunčiami el. laiškai, kurių darbuotojas nesiuntė, sistemos langai ar naršyklės atsidaro automatiškai, be vartotojo veiksmų, rodomi įspėjimai, reklamos ar kiti netipiniai pranešimai,
- pastebimas padidėjęs ar neįprastas tinklo srautas iš kompiuterinės darbo vietos,
- registruojamas neįprastas prisijungimų aktyvumas (pvz., iš neįprastų IP adresų, ne darbo metu),
- žurnaluose fiksuojami bandymai vykdyti neleistinas operacijas ar naudotis nesuteiktomis teisėmis,
- vykdomi neautorizuoti sistemos nustatymų keitimai ar diegiami įtartini programiniai komponentai ir kt.

14. Visus iš fizinių ar juridinių asmenų gautus pranešimus apie galimus kibernetinius incidentus darbuotojai turi nedelsdami pranešti SOC.

15. Jei kibernetinio saugumo vadovui nepakanka informacijos patvirtinti ar paneigti įvykusio arba galėjusio įvykti kibernetinio incidento faktą ar įvertinti jo poveikį, mastą bei galimas pasekmes, jis dėl papildomos informacijos pateikimo kreipiasi į SOC specialistus, atsakingą administratorių, TIS administratorius ar kitus darbuotojus, kurie nedelsdami privalo pateikti prašomą informaciją.

16. Kibernetinio saugumo vadovas įvertinęs pateiktą informaciją, privalo ne vėliau kaip per 12 darbo valandų (skaičiuojant darbo valandas; jei pranešimas gautas nedarbo metu, terminas pradedamas skaičiuoti nuo kitos darbo dienos darbo valandų pradžios) patvirtinti arba paneigti Kibernetinio incidento nustatymo faktą bei vadovaudamasis Kibernetinio incidento poveikio nustatymo kriterijais, nurodytais Plano 3 priede, per 12 val. nuo nustatymo įvertinti pirminį kibernetinio incidento poveikį ir mąstą ir jei pakanka duomenų – Kibernetinio incidento kategoriją.

17. Atsakingas administratorius vertinimo metu imasi veiksmų, kad būtų išsaugoti Kibernetinio incidento įrašai, įrodymai (pvz., išsaugomas paveiktos darbo stoties atvaizdas, žurnaliniai, audito įrašai, ekrano vaizdai (angl. Screenshots) ir pan.), kurie yra reikalingi pagrindinei kibernetinio incidento priežasčiai ar grėsmei nustatyti bei užtikrina jų patikimumą, vientisumą ir prieinamumą. Kibernetinio saugumo vadovui ši informacija turi būti perduota nurodytu būdu.

18. Kibernetinio saugumo vadovas organizuoja Kibernetinio incidento tyrimą. Kibernetinio incidento tyrimą vykdo atsakingas administratorius ir (ar) SOC specialistas.

19. Vertinimo metu surenkama informacija apie kibernetinį incidentą ir parengiama pirminė kibernetinio incidento vertinimo ataskaita. Įvertinęs surinktą informaciją, kibernetinio saugumo vadovas parengia ir teikia Kibernetinio incidento vertinimo ataskaitą Lietuvos vyriausiam archyvarui, TIS savininkui ir, jei incidentas susijęs su valstybės archyvu, šio archyvo direktoriui bei NKSC.

20. Kibernetinio saugumo vadovas saugo visą surinktą informaciją skaitmeninės informacijos saugojimo ir dalijimosi platformoje ir nuolat atnaujina informaciją apie atliktus veiksmus.

IV SKYRIUS
INFORMAVIMAS APIE KIBERNETINIUS INCIDENTUS

21. Kibernetinio saugumo vadovas įvertina poreikį informuoti Plano 2 priede nurodytus asmenis ir pranešti NKSC, registruodamas incidentą Nacionalinėje kibernetinių incidentų valdymo platformoje (https://incidentai.nksc.lt/) arba kitais NKSC nurodytais būdais. Apie didelio poveikio kibernetinį incidentą visuomet informuojami Plano 2 priede nurodyti asmenys ir NKSC. Apie nedidelio – informuojamas NKSC ir pagal poreikį Plano 2 priede nurodyti asmenys. Kiti darbuotojai ir (ar) informacinių sistemų naudotojai apie kibernetinį incidentą informuojami pagal situaciją ir atliekamas funkcijas.

22. Jei nustatomas didelio poveikio kibernetinis incidentas:

22.1. Kibernetinio saugumo vadovas nedelsiant, bet ne vėliau kaip per 24 valandas nuo jo nustatymo, teikia ankstyvąjį perspėjimą NKSC.

22.2. Ankstyvajame perspėjime apie kibernetinį incidentą nurodama ši turima pirminė informacija:

22.2.1. kibernetinio incidento apibūdinimas;

22.2.2. data ir laikas, kada kibernetinis incidentas įvyko ar buvo nustatytas;

22.2.3. vieta, įranga ar informacinė sistema, kur kibernetinis incidentas įvyko ar buvo nustatytas;

22.2.4. ar kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai;

22.2.5. ar kibernetinis incidentas galėtų daryti tarpvalstybinį poveikį; jei taip – nurodyti galimą tarpvalstybinį poveikį;

22.2.6. nurodyti dėl kibernetinio incidento paveiktas paslaugas, kurios patyrė ar gali patirti sutrikimų, ir sutrikimų apimtis (pirminiu vertinimu);

22.2.7. ar dėl kibernetinio incidento patirti ar gali būti patirti finansiniai nuostoliai, jei taip – nurodyti galimą finansinių nuostolių dydį;

22.2.8. ar kibernetinis incidentas paveikė ar gali paveikti kitus asmenis, sukeldamas turtinę arba neturtinę žalą; jei taip – nurodyti galimai paveiktus asmenis ir žalos dydžius;

22.2.9. ar kibernetinį incidentą sukėlė trečiosios šalys; jei taip – nurodyti galimas trečiąsias šalis;

22.2.10. turimi neteisėtų ar piktavališkų veiksmų įrodymai (jei tokių yra);

22.2.11. ar kibernetinis incidentas suvaldytas;

22.2.12. ar reikalinga pagalba suvaldant kibernetinį incidentą, jei taip – nurodyti galimos pagalbos priemones ir veiksmus;

22.2.13. ar kibernetinis incidentas pasikartoja;

22.2.14. ar apie kibernetinį incidentą buvo informuotos kitos įstaigos; jei taip – nurodyti įstaigas kurios buvo informuotos;

22.2.15. kita svarbi informacija.

22.3. Kibernetinio saugumo vadovas nedelsiant, bet ne vėliau kaip per 72 valandas nuo kibernetinio incidento nustatymo, atnaujina 22.2 papunktyje nurodytą informaciją ir nurodo incidento poveikį, atsižvelgdamas į tai:

22.3.1. ar paslaugos trikdomos visoje Lietuvos teritorijoje ir (ar) bent vienoje ES arba NATO šalyje;

22.3.2. ar tinklų ir informacinės sistemos veikla trikdoma 2 ar daugiau valandų;

22.3.3. ar paveiktų paslaugų gavėjų ar kompiuterizuotų darbo vietų skaičius lygus arba didesnis nei 1 000, arba 25 procentai (atsižvelgiant į tai, kuris dydis yra mažesnis);

22.3.4. ar paveikti 1 000 arba 25 procentų (atsižvelgiant į tai, kuris dydis yra mažesnis) paslaugų gavėjų asmens duomenys ar kiti kibernetinio saugumo subjekto saugomi paslaugų gavėjų duomenys;

22.3.5. ar valstybinės archyvų sistemos įstaiga nebegali užtikrinti teisės aktuose jos veiklai nustatytų reikalavimų įgyvendinimo;

22.3.6. ar yra prarastos arba atskleistos komercinės paslaptys arba įslaptinta informacija;

22.3.7. ar per 6 mėnesius patiriamas daugiau nei vienas analogiškas kibernetinis incidentas, incidentų pagrindinė priežastis sutampa ir patiriama ar galima patirti didelių finansinių nuostolių, lygių arba didesnių nei 500 000 Eur, arba 5 procentų kibernetinio saugumo subjekto praėjusių finansinių metų apyvartos (atsižvelgiant į tai, kuri suma yra mažesnė);

22.3.8. ar valstybinės archyvų sistemos įstaiga patiria ar gali patirti didelių finansinių nuostolių, lygių arba didesnių nei 500 000 Eur arba 5 procentų kibernetinio saugumo subjekto praėjusių finansinių metų apyvartos (atsižvelgiant į tai, kuri suma yra mažesnė);

22.3.9. ar bus atnaujinti ankstyvojo perspėjimo duomenys; jei taip – juos reikia atnaujinti ir NKSC platformoje pagal 22.2 papunktį;

22.3.10. ar kibernetinis incidentas sukėlė poveikį valstybinės archyvų sistemos įstaigos reputacijai; jei taip, – kokį;

22.3.11. data ir laikas, kada paslaugų teikimo sutrikimas buvo pašalintas;

22.3.12. ar kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą; jei taip:

22.3.12.1. ar galimos turtinės žalos dydis yra lygus arba didesnis nei 400 bazinių socialinių išmokų;

22.3.12.2. ar galimos neturtinės žalos dydis lygus arba didesnis nei 10 000 Eur;

22.3.12.3. ar sutrikdyta bent vieno žmogaus sveikata arba bent vienas žmogus žuvo;

22.3.13. ar kibernetinis incidentas suvaldytas; jei ne – kokios priemonės ar veiksmai bus atlikti siekiant jį suvaldyti;

22.3.14. kita svarbi informacija.

22.4. Kibernetinio saugumo vadovas per vieną mėnesį nuo pranešimo apie kibernetinį incidentą registravimo dienos teikia NKSC galutinę ataskaitą apie kibernetinį incidentą, joje pateikdamas 26 punkte nurodytą informaciją. Jeigu galutinės ataskaitos pateikimo metu kibernetinis incidentas tebevyksta, pateikiama pažangos ataskaita, o galutinė ataskaita – per vieną mėnesį nuo dienos, kai kibernetinis incidentas buvo suvaldytas.

22.5. NKSC prašymu per nurodytą terminą teikiama tarpinė atitinkamų atnaujintų padėties duomenų ataskaita;

22.6. Nustačius didelio poveikio kibernetinį incidentą, kibernetinio saugumo vadovas nedelsdamas informuoja VTVG vadovą, kuris įvertina poreikį aktyvuoti Veiklos tęstinumo valdymo planą;

23. Jei nustatomas nedidelio poveikio kibernetinis incidentas, kibernetinio saugumo vadovas nedelsiant, bet ne vėliau kaip per 72 valandas nuo jo nustatymo, teikia informaciją NKSC, nurodydamas šią informaciją:

23.1. kibernetinio incidento apibūdinimas;

23.2. data ir laikas, kada kibernetinis incidentas įvyko ar buvo nustatytas;

23.3. vieta, įranga ar informacinė sistema, kur ir kaip kibernetinis incidentas įvyko ar buvo nustatytas;

23.4. ar kibernetinis incidentas paveikė ar gali paveikti kitus asmenis, sukeldamas turtinę arba neturtinę žalą; jei taip – nurodyti, kas tie paveikti asmenys ir koks žalos dydis;

23.5. ar kibernetinis incidentas suvaldytas; jei ne – nurodomos priemonės ar veiksmai, kurie bus atlikti siekiant suvaldyti kibernetinį incidentą;

23.6. ar kibernetinį incidentą, kaip įtariama, sukėlė neteisėti ar piktavališki veiksmai; jei taip – kokie;

23.7. dėl kibernetinio incidento paveiktos paslaugos, kurios patyrė ar gali patirti sutrikimų, sutrikimų apimtys;

23.8. ar dėl kibernetinio incidento patirti ar gali būti patirti finansiniai nuostoliai; jei taip – koks nuostolių dydis;

23.9. ar kibernetinį incidentą sukėlė trečiosios šalys; jei taip – kokios trečiosios šalys;

23.10. nurodyti turimus neteisėtus ar piktavališkus veiksmų įrodymus (jei tokių yra);

23.11. ar kibernetinis incidentas galėtų daryti tarpvalstybinį poveikį; jei taip, nurodyti galimą tarpvalstybinį poveikį;

23.12. ar reikalinga pagalba suvaldant kibernetinį incidentą;

23.13. ar apie kibernetinį incidentą buvo informuotos kitos įstaigos; jei taip – kokios įstaigos buvo informuotos;

23.14. ar bus teikiama galutinė kibernetinio incidento ataskaita; jei ne, pateikiama 26 punkte nurodyta informacija;

23.15. kita svarbi informacija.

24. Kibernetinio saugumo vadovas per vieną mėnesį nuo pranešimo apie kibernetinį incidentą registravimo dienos teikia galutinę ataskaitą apie nedidelį kibernetinį incidentą, joje pateikdamas 26 punkte nurodytą informaciją. Galutinė ataskaita apie nedidelį kibernetinį incidentą neteikiama, jei pranešime apie kibernetinį incidentą pateikta visa galutinės ataskaitos informacija.

25. Jei nustatomas vos neįvykęs kibernetinis incidentas, kibernetinio saugumo vadovas gali apie jį pranešti NKSC, pateikdamas trumpą suvestinę:

25.1. vieta, įranga ar informacinė sistema, kur ir kaip kibernetinis incidentas vos neįvyko ar buvo nustatytas;

25.2. trumpas pranešimas apie vos neįvykusių incidentą;

25.3. kita svarbi informacija.

26. Galutinėje kibernetinio incidento valdymo ataskaitoje nurodama ši informacija:

26.1. kibernetinė grėsmė pagal Plano 6 priede pateiktą sąrašą;

26.2. Išsamus kibernetinio incidento, įskaitant jo sunkumą ir poveikį, aprašymas;

26.3. taikomos ir įgyvendinamos kibernetinio incidento poveikio mažinimo priemonės.

V SKYRIUS
KIBERNETINIO INCIDENTO SUSTABDYMAS IR SUVALDYMAS

27. Atsižvelgiant į nustatytą kibernetinį incidentą ir esamą poveikį, kibernetinio saugumo vadovas nustato kibernetinio incidento valdymo prioritetus. Jei nenuspręsta kitaip, pirmiausiai valdomi didžiausią poveikį turintys kibernetiniai incidentai.

28. Kibernetinis incidentas laikomas sustabdytu, kai jo būsena iš aktyvios tampa pasyvia. Kibernetinis incidentas laikomas suvaldytu, kai jis yra sustabdytas ir pašalintas pažeidžiamumas (spraga) bei nenustatyta papildomo išplitimo ir (ar) neigiamo poveikio TIS veiklai.

29. Jei nustatomas nedidelio poveikio kibernetinis incidentas:

29.1. kibernetinio saugumo vadovas kartu su SOC specialistais ir (ar) atsakingu administratoriumi, atsižvelgdamas į incidento tipą, poveikį ir galimas jo valdymo priemones, parenka ir taiko efektyviausią galimą kibernetinio incidento valdymo priemonę (stabdymą, šalinimą, pažeidžiamumo ir incidento pašalinimą);

29.2. Atsakingas administratorius ir SOC specialistas informaciją apie kibernetinio incidento stabdymą, pažeidžiamumo pašalinimo priemones bei kibernetinio incidento tyrimo eigą teikia kibernetinio saugumo vadovui ne rečiau kaip kas 12 valandų, iki kibernetinis incidentas bus suvaldytas ar pasibaigs.

30. Jei nustatomas didelio poveikio Incidentas:

30.1. Kibernetinio saugumo vadovas, esant poreikiui susiderinęs su Atsakingu administratoriumi ir (ar) SOC specialistu, informuoja Aprašo 2 priede nurodytus asmenis apie planuojamas taikyti Incidento valdymo priemones (stabdymą – paskyrų ir (ar) paslaugų sustabdymą, tinklo apribojimą, kompiuterinės darbo vietos izoliavimą, tinklo srauto filtravimą ir pan., incidento šalinimo eigą, pažeidžiamumo pašalinimą, papildomų apsaugų – užkardų, incidentų prevencijos sistemų, slaptažodžių papildomos apsaugos priemonių – diegimą).

30.2. Siekiant suvaldyti Incidentą ir atkurti įprastą Archyvų TIS veiklą, Aprašo 2 priede nurodyti asmenys, atlikdami savo funkcijas, imasi visų galimų organizacinių, techninių ir teisinių priemonių (toliau – Incidento valdymo priemonės).

30.3. Pagrindiniai kriterijai, kuriais vadovaujantis priimamas sprendimas dėl Incidento valdymo priemonių:

30.3.1. Plano 2 priede nurodyti asmenys teikia pasiūlymus dėl kibernetinio incidento valdymo;

30.3.2. įvertinamas galimas poveikis ir žala valstybinės archyvų sistemos įstaigai;

30.3.3. nustatomas maksimalus valstybinės archyvų sistemos įstaigos TIS priimtinas neveikimo laikas (MTPD);

30.3.4. numatomas kibernetinio incidento valdymo sprendimui įgyvendinti reikalingas laikas ir ištekliai;

30.3.5. numatomos kitos rizikos, galinčios kilti dėl kibernetinio incidento, priėmus jo valdymo sprendimą;

30.3.6. įvertinamos NKSC ir kompetentingų institucijų rekomendacijos.

30.4. Atsakingas administratorius nedelsdamas imasi reikiamų priemonių, kad kibernetinis incidentas būtų sustabdytas, ir informuoja kibernetinio saugumo vadovą, kai kibernetinis incidentas sustabdomas.

30.5. Atsakingas administratorius ir SOC specialistas per kuo trumpesnį laiką nuo Kibernetinio incidento sustabdymo imasi priemonių kibernetiniam incidentui bei pažeidžiamumui, dėl kurio jis įvyko, nustatyti ir pašalinti bei informuoja kibernetinio saugumo vadovą, kai kibernetinis incidentas ir pažeidžiamumas yra pašalinti.

30.6. Kibernetinio saugumo vadovas įvertinęs, kad kibernetinio incidento nepavyks ištirti ir (ar) suvaldyti patiems, informuoja Plano 2 priede nurodytus asmenis dėl kreipimosi tarnybinės pagalbos į NKSC su prašymu padėti atlikti kibernetinio incidento tyrimą ir valdymą.

30.7. Iki kibernetinis incidentas bus suvaldytas ar pasibaigs, kibernetinio saugumo vadovas Plano 2 priede nurodytiems asmenims atnaujintą informaciją teikia ne rečiau kaip kas 24 valandas, o NKSC – NKSC nurodytais terminais, bet ne rečiau kaip kas 24 valandas, jei siekiama suvaldyti didelio poveikio kibernetinį incidentą. Valdymo ataskaita teikiama pagal Plano 26 punkte nustatytus reikalavimus.

30.8. Atsakingas administratorius ir SOC specialistas informaciją apie kibernetinio incidento stabdymą, pažeidžiamumo pašalinimo priemones bei kibernetinio incidento tyrimo eigą teikia kibernetinio saugumo vadovui ne rečiau kaip kas 12 valandų, iki kibernetinis incidentas bus suvaldytas ar pasibaigs.

30.9. Suvaldžius kibernetinį incidentą, kibernetinio saugumo vadovas ne vėliau kaip per keturias valandas nuo kibernetinio incidento suvaldymo ar jo pabaigos apie kibernetinio incidento suvaldymo rezultatus informuoja Plano 2 priede nurodytus asmenis ir NKSC.

31. Suvaldžius kibernetinį incidentą, kibernetinio saugumo vadovas Kibernetinių incidentų registravimo žurnale užfiksuoja incidento suvaldymo datą ir laiką bei pateikia kitą papildomą informaciją, numatytą Plano 26 punkte.

VI SKYRIUS

INCIDENTŲ TYRIMAS

32. Kibernetinio incidento tyrimą organizuoja kibernetinio saugumo vadovas.

33. Kibernetinio incidento tyrimo metu atsakingas administratorius, SOC specialistas ar kiti tyrime dalyvaujantys asmenys (toliau – kibernetinio incidento tyrėjai), siekdami surinkti įrodymus ir nustatyti visas su kibernetiniu incidentu susijusias aplinkybes, turi teisę gauti iš valstybinės archyvų sistemos įstaigos darbuotojų įstaigai priklausančius įrenginius, kuriuose įvyko kibernetinis incidentas.

34. Įrenginiuose, kuriuose įvyko kibernetinis incidentas, neatliekami jokie aktyvūs tyrimo veiksmai. Tyrimas vykdomas analizuojant surinktus techninius įrodymus: žurnalinius (audito) įrašus, įrenginio disko atvaizdą, aktyviosios atminties atvaizdą, tinklo srauto duomenis ir kitus tyrimui naudingus duomenis.

35. Surinktos tyrimo medžiagos pagrindu kibernetinio incidento tyrėjai parengia Kibernetinio incidento tyrimo atskaitą, kurioje išdėsto kibernetinio incidento aplinkybes ir jas pagrindžiančius faktus (data, laikas, incidento šaltinis, naudotojo veiksmų seka ir aplinkybės, tokios kaip gavimo šaltinis, spaustas nuorodos, parsisiųsti failai ir pan.), kibernetinio incidento veikimo požymius, pasekmes, išplitimo mastą, priemones, kuriomis kibernetinis incidentas nustatytas, priemones, kuriomis jis buvo valdomas, saugumo spragą, kuria buvo pasinaudota, ir pan.) ir visą kitą informaciją, nurodytą Plano 26 punkte. Ši ataskaitą teikiama kibernetinio saugumo vadovui.

36. Kibernetinio incidento tyrėjams surinkus ir pateikus visą reikiamą tyrimo medžiagą, kibernetinio saugumo vadovas pateikia apibendrinančią išvadą ir priima sprendimą dėl kibernetinio incidento tyrimo pabaigos.

VII SKYRIUS
RYŠIŲ IR INFORMACINĖS INFRASTRUKTŪROS VEIKLOS ATKŪRIMAS IR KIBERNETINIO INCIDENTO ANALIZĖ

37. TIS veiklos atkūrimą atsakingas administratorius vykdo tik suvaldžius kibernetinį incidentą.

38. Kibernetinio saugumo vadovas gauna patvirtinimą iš atsakingo administratoriaus, kad TIS atkurta, pažeidžiamumas pašalintas.

39. Kibernetinio saugumo vadovas apie atkurtą veiklą ir pašalintą pažeidžiamumą informuoja NKSC.

40. Viešųjų ryšių atstovas, jei buvo informuotas apie kibernetinį incidentą, informuoja TIS naudotojus ir (ar) visuomenę apie kibernetinio incidento suvaldymą ir atkurtas paslaugas.

41. Suvaldžius kibernetinį incidentą ar jam pasibaigus:

41.1. didelio poveikio incidento atveju kibernetinio saugumo vadovas ne vėliau kaip per penkias darbo dienas nuo incidento suvaldymo valstybinės archyvų sistemos

įstaigoje organizuoja įvykusio kibernetinio incidento analizę. Analizėje dalyvauja Plano 2 priede nurodyti asmenys ir pagal poreikį kiti valstybinės archyvų sistemos įstaigos darbuotojai.

41.2. Kibernetinio incidento analizės metu įvertinamas poreikis peržiūrėti kibernetinį saugumą reglamentuojančias procedūras ir, jei reikia, atitinkamai pakeisti šią sritį reglamentuojančius įstaigos vidaus teisės aktus, aptariamos kibernetinio incidento valdymo metu iškilusios problemos ir pan.

41.3. Kibernetinio saugumo vadovas, vadovaudamasis Plano 22.4 ar 23.16 papunkčiais, pateikia NKSC Kibernetinio incidento tyrimo ir valdymo ataskaitą – susistemintą ir aktualią neįslaptintą, nuasmenintą informaciją apie kibernetinio incidento nustatymą ir suvaldymą. Tyrimo ir valdymo ataskaita registruojama dokumentų valdymo sistemoje.

41.4. Kibernetinio saugumo vadovas kibernetinio saugumo informacinės sistemos (toliau – KSIS) priemonėmis su KSIS nariais pasidalija kibernetinio incidento tyrimo metu surinktais indikatoriais.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

42. Darbuotojai, dėl kurių neteisėtų veiksmų ar neveikimo įvyko kibernetinis incidentas, atsako teisės aktų nustatyta tvarka.

43. Kibernetinių incidentų registravimo žurnalas ir kibernetinių incidentų tyrimų dokumentai saugomi 3 metus.

44. Kibernetinio saugumo vadovas kiekvienais metais organizuoja šio Plano veiksmingumo bandymą, imituodamas kibernetinį incidentą ir įtraukdamas jo valdymo veikloje dalyvaujančius asmenis į būtinus tokiomis aplinkybėmis veiksmus.

45. Šis Planas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba įvykus esminiai pokyčių, galinčių turėti įtakos šiam Planui. Už šio Plano peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas. Planas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

_____

Kibernetinių incidentų
valdymo plano
1 priedas

(Apskaitos žurnalo forma)

KIBERNETINIŲ INCIDENTŲ VALDYMO PLANO PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	**Veiklos data**	**statusas**	**Atsakingas asmuo**	**Pagrindinės korekcijos**	**Patvirtinimo data ir Nr.**

_____

Kibernetinių incidentų
valdymo plano
2 priedas

(Kibernetinio incidento valdymo procese dalyvaujančių atsakingų asmenų ir institucijų sąrašų ir kontaktų forma)

KIBERNETINIO INCIDENTO VALDYMO PROCESE DALYVAUJANČIŲ ATSAKINGŲ ASMENŲ IR INSTITUCIJŲ KONTAKTAI

Nr.	Pareigos/ Institucija	Vardas, pavardė	El. paštas	Telefonas	Interneto svetainė

_____

Kibernetinių incidentų
valdymo plano
3 priedas

KRITERIJAI, KURIAIS VADOVAUJANTIS KIBERNETINIAI INCIDENTAI PRISKIRIAMI DIDELIAM KIBERNETINIAM INCIDENTUI

Nr.	Poveikio kriterijus	Pavyzdžiai
1.	Paslaugos trikdomos visoje Lietuvos teritorijoje ir (ar) bent vienoje ES arba NATO šalyje	-
2.	Tinklų ir informacinės sistemos veikla trikdoma 2 ar daugiau valandų	Ilgiau nei 2 val. nepasiekiamos svetainės ar jų dalis: - *.archyvai.lt - eais.archyvai.lt - adoc.archyvai.lt - epartizanai.archyvai.lt - lyavaizdai.archyvai.lt, - lyapavardes.archyvai.lt, - virtualios-parodos.archyvai.lt - diaspora.archyvai.lt - eais.archyvai.lt, - eais-int.archyvai.lt - eais-test.archyvai.lt, - adoc.archyvai.lt, - eais-pub.archyvai.lt

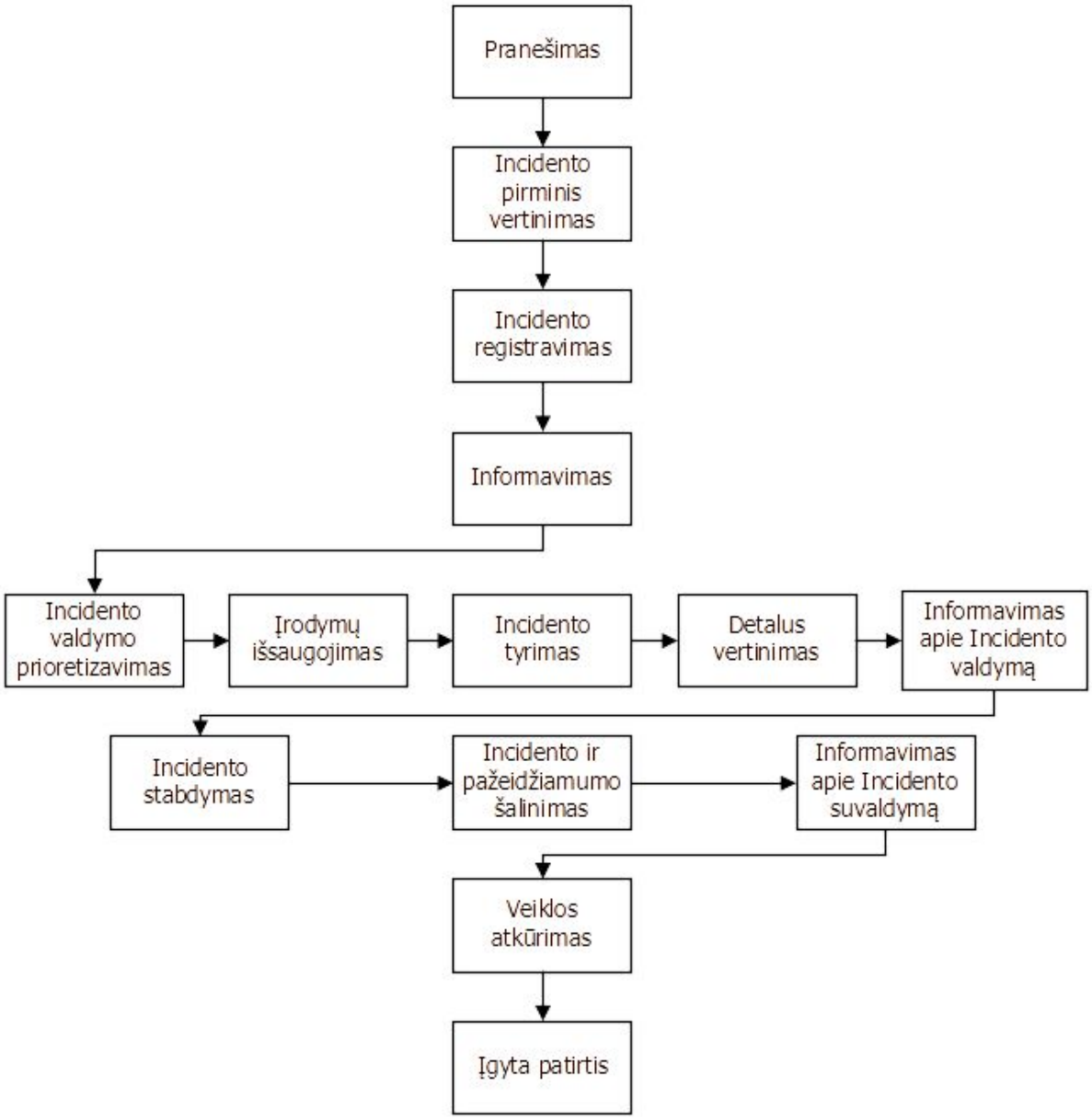
		- eais-isr.archyvai.lt Neveikia EAIS, informacinės sistemos E. Kinas funkcionalumai, neveikia el. paštas.
3.	Paveiktų paslaugų gavėjų ar kompiuterizuotų darbo vietų skaičius lygus arba didesnis nei 1 000 arba 25 procentai (atsižvelgiant į tai, kuris dydis yra mažesnis)	- 25 proc. subjektų negali pateikti skaitmeninės kilmės ir suskaitmenintų dokumentų, ISR duomenų į EAIS sistemą; - paveikta 25 proc. valstybinės archyvų sistemos įstaigos kompiuterinių darbo vietų.
4.	Paveikti 1 000 arba 25 procentų (atsižvelgiant į tai, kuris dydis yra mažesnis) paslaugų gavėjų asmens duomenys ar kiti kibernetinio saugumo subjekto saugomi paslaugų gavėjų duomenys	- Atskleisti, sunaikinti mažiausiai 25 proc. visų turimų asmens duomenų EAIS, informacinėje sistemoje E. Kinas ar kitose IT sistemose. -
5.	Kibernetinio saugumo subjektas negali užtikrinti teisės aktuose jo veiklai nustatytų reikalavimų įgyvendinimo	- Archyvai negali teikti juridinius faktus patvirtinančių dokumentų, pažymų ir elektroninių dokumentų kopijų užsakymo elektroninių paslaugų. -
6.	Prarastos arba atskleistos komercinės paslaptys arba įslaptinta informacija	- Sunaikinti arba paviešinti nevieši valstybinės archyvų sistemos įstaigų ar sistemų kaupiami duomenys.
7.	Per 6 mėnesius patiriamas daugiau nei vienas analogiškas kibernetinis incidentas, incidentų pagrindinė priežastis sutampa ir patiriama ar galima patirti didelių finansinių nuostolių	
8	Kibernetinio saugumo subjektas patiria ar gali patirti didelių finansinių nuostolių, lygių arba didesnių nei 500 000 Eur	Užšifruota EAIS, informacinė sitema E. Kinas.

9	Kibernetinis incidentas paveikė arba gali paveikti kitus fizinius ar juridinius asmenis, sukeldamas didelę turtinę arba neturtinę žalą, atitinkančią bent vieną iš šių kriterijų: - galimos turtinės žalos dydis yra lygus arba didesnis nei 400 bazinių socialinių išmokų; - galimos neturtinės žalos dydis lygus arba didesnis nei 10 000 Eur; - sutrikdyta bent vieno žmogaus sveikata arba bent vienas žmogus žuvo.	-

_____

Kibernetinių incidentų
valdymo plano
4 priedas

KIBERNETINIO INCIDENTO VALDYMO SCHEMA



Kibernetinių incidentų
valdymo plano
5 priedas

PAGRINDINIAI ŠALTINIAI, KURIAIS NAUDOJANTIS GALI BŪTI SUKELTAS KIBERNETINIS INCIDENTAS, IR JŲ APRAŠYMAS

Kibernetinio incidento šaltinis	**Aprašymas**
Išorinės kompiuterinės laikmenos	Kibernetinė ataka gali būti įvykdyta ir išplisti sistemose per nesaugias ar užkrėstas išorines laikmenas (USB, CD, nešiojamuosius HDD ir t. t.).
Interneto svetainių pagrindu veikianti programinė įranga	Kibernetinė ataka gali būti įvykdyta lankantis nesaugioje interneto svetainėje ar kitoje interneto svetainės pagrindu veikiančioje aplikacijoje. Kenkėjiška interneto svetainė, pasinaudodama vienu iš atakos būdų, gali perimti naudotojo sesijas ir prisijungimo duomenis, nukreipti naudotoją į apgaulingą puslapį arba bandyti išnaudoti naudotojo naršyklės pažeidžiamą, kad galėtų užvaldyti jo kompiuterį.
El. paštas ir socialiniai tinklai	Kibernetinė ataka gali būti įvykdyta atvėrus el. pašto laišką su kenkėjišku priedu arba aktyvavus kenkėjišką nuorodą. Pasinaudojant socialinės inžinerijos atakos principais gali būti siekiama, kad laiško gavėjas atvertų kenkėjišką failą (dažnu atveju su plėtiniu .exe), sudarydamas galimybes užvaldyti jo kompiuterį ar pavogti prisijungimo ir kitus jautrius duomenis.
Netinkamai valdoma prieiga prie viešai pasiekiamų resursų	Kibernetinė ataka gali būti įvykdyta, jei sistemos viešai pasiekiami resursai (autentifikacija) nėra tinkamai apsaugoti ir kibernetinis nusikaltėlis brutalios jėgos būdu ar pasinaudodamas žodyno tipo ataka gali atspėti prisijungimo duomenis ir prisijungęs prie sistemos ją užvaldyti.
Prarasta įranga	Kibernetinė ataka gali būti įvykdyta praradus įrangą, kurios duomenys nešifruoti (nešiojamąjį kompiuterį, telefoną ir t.t.). Prarasta įranga gali būti panaudota slaptažodžiams išgauti, neteisėtai prieigai prie jautrių duomenų.
Kiti kibernetinių incidentų šaltiniai	Kitokio pobūdžio kibernetiniai nusikaltimai, kurie nebuvo išvardyti.

_____

Kibernetinių incidentų
valdymo plano
6 priedas

**KIBERNETINIŲ GRĖSMIŲ IR
PAGRINDINIŲ INCIDENTŲ PRIEŽASTYS**

1. Nepageidaujamų laiškų ir (ar) klaidinančios ar žeidžiančios informacijos platinimas (angl. *abusive content*, *spam*) ir (ar) tinklų informacinės sistemos veiklos trikdymas.
2. Kenkimo programinė įranga (angl. *malicious software / code*): programinė įranga ar jos dalis, kuri padeda neteisėtai prisijungti prie tinklų ir informacinės sistemos, ją užvaldyti ir kontroliuoti, sutrikdyti ar pakeisti jos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti skaitmeninius duomenis, panaikinti ar apriboti galimybę jais naudotis ir neteisėtai pasisavinti ar kitaip panaudoti neviešus skaitmeninius duomenis tokios teisės neturintiems asmenims ir kuri identifikuota kaip:
2.1. pažangi kenkimo programinė įranga (angl*. advanced persistent threat, APT*);
2.2. tinklų ir informacinės sistemos duomenis šifruojantis ir naikinantis (angl. *wiper*) ar išpirkos reikalaujantis programinis kodas (angl. *ransomware*);
2.3. tinklų ir informacinės sistemos dalys, aktyviai kontroliuojamos įsibrovėlių;
2.4. kenkimo programinės įrangos platinimas.
3. Informacijos rinkimas (angl. *information gathering*): žvalgyba ar kita įtartina veikla, manipuliavimas naudotojų emocijomis, psichologija, pastabumo stoka, pasinaudojimas technologiniu neišmanymu (angl. *social engineering*), siekiant stebėti ir rinkti informaciją, atrasti silpnąsias vietas, atlikti grėsmę keliančius veiksmus, apgavystės, siekiant įtikinti naudotoją atskleisti informaciją (angl. *phishing*) arba atlikti norimus veiksmus. Naudojami socialinės inžinerijos metodai, siekiant išvilioti prisijungimo prie tinklų ir informacinės sistemos ir (ar) kitą svarbią informaciją.
4. Mėginimas įsilaužti (angl. *intrusion attempts*). Mėginimas įsilaužti arba sutrikdyti tinklų ir informacinės sistemos veikimą išnaudojant žinomas spragas (angl. *exploiting of known vulnerabilities*), bandant parinkti slaptažodžius (angl. *login attempts*), kitą įsilaužimo būdą (angl. *new attack signature*), kurie gali būti skirstomi į:
4.1. išnaudojama viena ar kelios nežinomos spragos (angl. *zero day*);
4.2. tinklų ir informacinės sistemos žvalgyba ar kita kenkimo veika (prievadų skenavimas, slaptažodžių parinkimas, kenkimo programinės įrangos platinimas ir kita);
4.3. išnaudojamos žinomos ir viešai publikuotos spragos.
5. Įsilaužimas (angl. *intrusions*). Sėkmingas įsilaužimas ir (ar) neteisėtas tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos naudojimas (angl. *privileged account compromise, unprivileged account compromise, application compromise*), kuris skirstomas taip:

5.1. veiksmai prieš tinklų ir informacinę sistemą ar jos saugumo priemones, informacijos pasisavinimas, naikinimas, tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis tinklų ir informacinės sistemos teikiamų paslaugų nepertraukiamą teikimą, galintis turėti įtakos tvarkomos informacijos ir teikiamų paslaugų patikimumui, iškreipti turinį ir mažinti tinklų ir informacinės sistemos naudotojų pasitikėjimą jais;
5.2. gaunama neteisėta prieiga prie tinklų ir informacinės sistemos, taikomosios programinės įrangos ar paslaugos.
6. Paslaugų trikdymas, prieinamumo pažeidimai (angl. *availability*): veiksmai, kuriais trikdoma tinklų ir informacinės sistemos veikla, teikiamos paslaugos (angl. *DoS, DDoS*), tinklų ir informacinės sistemos ar jos dalies pažeidimas, sutrikdantis tinklų ir informacinės sistemos ir (ar) jos teikiamas paslaugas, kuris skirstomas taip:
6.1. teikiamų paslaugų nutraukimas arba maksimalaus leistino paslaugos neveikimo laiko viršijimas;
6.2. teikiamų paslaugų nepertraukiamo teikimo trikdymas, galintis turėti įtakos tvarkomos informacijos ir (ar) teikiamų paslaugų prieinamumui.
7. Tiekimo grandinės atakos (angl. *supply chain attack*): išnaudojama trečiųjų šalių, teikiančių paslaugas tinklų ir informacinės sistemos valdytojui ir (ar) tvarkytojui, infrastruktūra, siekiant įgauti ar turėti įtakos paslaugos gavėjo tinklų ir informacinės sistemos infrastruktūrai.
8. Informacijos turinio saugumo pažeidimai (angl. *information content security*): neteisėta prieiga prie informacijos, galinčios turėti įtakos tinklų ir informacinės sistemos veiklai ir (ar) teikiamoms paslaugoms, ar jos neteisėtas keitimas.
9. Neteisėta veikla, sukčiavimas (angl. *fraud*): vagystė, apgavystė, neteisėtas išteklių (angl. *unauthorized use of resources*), nelegalios programinės įrangos ar autorių teisių (angl. *copyright*) naudojimas, tapatybės klastojimo, apgavystės ir kiti panašaus pobūdžio incidentai.
10. Kitos grėsmės ar priežastys.

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

ŽURNALINIŲ ĮRAŠŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Žurnalinių įrašų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) žurnalinių įrašų rinkimą, saugojimą, analizavimą ir ištrynimą bei šių procesų auditavimą.

2. Apraše vartojamos sąvokos:

2.1. **Kibernetinio saugumo vadovas**– asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

2.2. **Saugumo operacijų centras** (toliau – SOC) – Lietuvos vyriausiojo archyvaro ar jo įgalioto asmens paskirtas asmuo ar grupė, taip pat paslaugas teikianti trečioji šalis, atsakinga už žurnalinių įrašų ir kibernetinių incidentų stebėjimą ir valdymą;

2.3. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

2.4. **Žurnaliniai įrašai** (angl. *log files*) – tai įrašai, kuriuose sistemingai fiksuojama informacija apie įvairius tinklų ir informacinių sistemų įvykius, veiksmus ar būsenas valstybinės archyvų sistemos įstaigose. Šie įrašai leidžia atsekti sistemų veiklą, analizuoti incidentus, identifikuoti grėsmes ir užtikrinti atitiktį teisės aktų nustatytiems reikalavimams.

3. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

4. Jei SOC paslaugas teikia trečiųjų šalių paslaugų teikėjai, šis Aprašas turi būti pateiktas paslaugų teikėjui.

II SKYRIUS
FUNKCIJOS IR ATSAKOMYBĖS

5. Šiame Apraše numatytos SOC funkcijos ir atsakomybės, susijusios su žurnalinių įrašų valdymu, yra pateiktos Kibernetinių incidentų valdymo plane.

6. Kibernetinio saugumo vadovo funkcijos ir atsakomybės:

6.1. koordinuoti šio Aprašo įgyvendinimą;

6.2. periodiškai peržiūrėti ir atnaujinti Aprašą;

6.3. užtikrinti žurnalinių įrašų valdymo atitiktį teisės aktų reikalavimams;

6.4. identifikuoti galimas rizikas, susijusias su žurnalinių įrašų valdymu;

6.5. inicijuoti techninių priemonių, skirtų žurnalinių įrašų rinkimui ir analizei, tinkamumo vertinimą ir tobulinimą;

6.6. peržiūrėti ir vertinti SOC pateiktų žurnalinių įrašų analizės ataskaitas bei identifikuoti problemas ir inicijuoti taisomuosius veiksmus;

6.7. dalyvauti diegiant ir prižiūrint techninius sprendimus, susijusius su žurnalinių įrašų fiksavimu, saugojimu ir analize;

6.8. vertinti, ar užtikrinamas TIS žurnalinių įrašų fiksavimas pagal šį Aprašą, ir, jei reikia, inicijuoti TIS konfigūracijos atnaujinimą.

7. TIS administratoriaus funkcijos ir atsakomybės:

7.1. stebėti, ar nepertraukiamai veikia žurnalinių įrašų surinkimo ir saugojimo funkcijos;

7.2. identifikuoti TIS trikdžius, pvz., žurnalinių įrašų nefiksavimą, nedelsiant apie juos informuoti SOC arba Kibernetinio saugumo vadovą;

7.3. bendradarbiauti su SOC teikiant informaciją apie žurnalinių įrašų šaltinius, konfigūracijas, veikimo aplinką ir palaikant jų techninį veikimą.

III SKYRIUS
ŽURNALINIŲ ĮRAŠŲ NAUDOJIMAS IR VALDYMAS

8. Valstybinės archyvų sistemos įstaigų žurnaliniai įrašai renkami, analizuojami ir naudojami TIS veiksnumo, jų naudotojų ir administratorių veiksmų auditui ir kontrolei bei kibernetinių incidentų tyrimui, siekiant:

8.1. nustatyti (atsekti) neteisėtus ar neleistinus veiksmus, atliekamus TIS (pvz., įvykus kibernetiniam incidentui, kai būtina ištirti jo atsiradimo priežastis);

8.2. fiksuoti TIS kylančias grėsmes ir gedimus;

8.3. išsaugoti techninės ir programinės įrangos klaidų pranešimus;

8.4. atitikti kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytus reikalavimus;

8.5. analizuoti žurnalinių įrašų duomenis, siekiant sumažinti kibernetinių incidentų įvykio tikimybę;

8.6. laiku pastebėti kibernetines grėsmes ir vykusius kibernetinius incidentus ir asmens duomenų saugumo pažeidimus.

9. Žurnaliniai įrašai yra saugomi 90 kalendorinių dienų. Jei žurnaliniuose įrašuose yra asmens duomenų, jų saugojimo ir sunaikinimo terminai turi būti nustatomi atsižvelgiant į 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, reikalavimus.

10. Naudojant technines ir organizacines priemones turi būti užtikrinamas žurnalinių įrašų konfidencialumas, vientisumas ir prieinamumas. Būtina užtikrinti kontrolės mechanizmus, sudarančius galimybes identifikuoti šių principų pažeidimus.

11. TIS žurnalinių įrašų valdymo procesas turi užtikrinti, kad žurnaliniai įrašai būtų fiksuojami laiku, renkami, analizuojami ir saugomi.

12. Žurnalinių įrašų generavimas ir surinkimas turi būti užtikrinami nepertraukiamai. Įrašų generavimui bei persiuntimui turi būti naudojamos sisteminės paslaugos ir įrankiai (pvz., Syslog, Sysmon, Windows Event Forwarding), įrašai turi būti kaupiami centriniame žurnalų surinkimo serveryje, o jų analizei pasitelkiama specializuota saugumo informacijos ir įvykių valdymo (angl. Security Information and Event Management – SIEM) programinė įranga.

13. Siekiant žurnalinių įrašų tikslumo, TIS turi turėti ne mažiau kaip 2 laiko šaltinius.

14. Priemonės, naudojamos vidinės TIS sąsajoje su viešųjų elektroninių ryšių tinklu, turi būti nustatytos taip, kad žurnaliniuose įrašuose fiksuotų visus įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais.

15. Dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant (jei tai įmanoma – automatiniu pranešimu), bet ne vėliau kaip per vieną darbo dieną turi būti informuojamas Kibernetinio saugumo vadovas.

16. Žurnalinius įrašus draudžiama trinti ar keisti, kol nėra pasibaigęs jų saugojimo terminas.

17. Žurnalinių įrašų kopijos turi būti apsaugotos nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo.

18. Naudojimasis žurnaliniais įrašais turi būti kontroliuojamas ir fiksuojamas, žurnaliniai įrašai turi būti pasiekiami tik TIS administratoriui, SOC ir Kibernetinio saugumo vadovui (peržiūros teisėmis).

19. Neįprasta veikla turi būti užfiksuojama žurnaliniuose įrašuose. SOC, atsižvelgdamas į valstybinės archyvų sistemos įstaigų veiklos pobūdį, struktūrą ir kibernetinių grėsmių aplinką, iš surinktų žurnalinių įrašų turi parengti taisykles ir sukonfigūruoti automatinius pranešimus, leidžiančius nustatyti reikšmingus nukrypimus ir galimas kibernetines atakas, bei taikyti jų analizę realiuoju arba beveik realiuoju laiku.

20. SOC analizuoja identifikuotus įtartinus TIS žurnalinius įrašus, kuriuose fiksuojami veiksmai, pvz. neautorizuota prieiga, bandymai apeiti saugumo mechanizmus, neįprasti naudotojų ar sistemų veiklos modeliai ir kt.

21. SOC, žurnalinių įrašų ir automatinių pranešimų analizės metu nustatęs galimus informacijos saugos incidentus, atlieka jų valdymą pagal Kibernetinių incidentų valdymo tvarkos aprašą.

22. SOC kas mėnesį Kibernetinio saugumo vadovui turi pateikti žurnalinių įrašų analizės apibendrintą ataskaitą.

IV SKYRIUS
ŽURNALINIŲ ĮRAŠŲ FIKSAVIMO NUOSTATOS

23. Turi būti fiksuojami bent jau šie žurnaliniai įrašai (jei TIS dalys palaiko tokį funkcionalumą):

23.1. TIS komponentų (serverių, virtualių serverių, saugasienių, maršrutizatorių,

komutatorių ir kitų subjekto identifikuotų svarbių komponentų) įjungimas, išjungimas ar perkrovimas;

23.2. naudotojų ir administratorių autentifikavimo įvykiai;

23.3. naudotojų, administratorių paskyrų sukūrimas, prieigų prie tinklų ir informacinių sistemų pakeitimai;

23.4. administratorių atliekami veiksmai;

23.5. operacinėse sistemose sukurti ir atlikti sisteminiai uždavinių įvykiai (angl. Scheduled task);

23.6. grupinių politikų pakeitimai;

23.7. saugasienių taisyklių pakeitimai;

23.8. žurnalinių įrašų rinkimo funkcijos įjungimas, išjungimas;

23.9. operacinių sistemų laiko ir datos pakeitimai;

23.10. saugumo sistemų (antivirusinių, įsibrovimo aptikimo sistemų) įjungimas ir išjungimas;

23.11. operacinėse sistemose vykstančių procesų ar servisų įvykiai;

23.12. TIS galinių įrenginių autentifikavimo įvykiai;

23.13. žurnalinių įrašų peržiūrėjimas, trynimas, kūrimas ar keitimas.

24. Žurnaliniuose įrašuose turi būti fiksuojami bent jau šie duomenys (jei TIS dalys palaiko tokį funkcionalumą):

24.1. įvykio data ir tikslus laikas;

24.2. įvykio rūšis (informacija, klaida, saugumo pranešimas, sisteminis pranešimas, perspėjimas (angl. *warning*));

24.3. naudotojo / administratoriaus ir (arba) TIS įrenginio, susijusio su įvykiu, identifikavimo duomenys;

24.4. įvykio šaltinio IP adresas (arba kitas tinklo identifikatorius);

24.5. įvykio rezultatas (sėkmingas / nesėkmingas);

24.6. įvykio aprašymas.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

25. Visi valstybinės archyvų sistemos įstaigų žurnalinių įrašų valdymo procese dalyvaujantys darbuotojai privalo laikytis šio Aprašo reikalavimų.

26. Aprašo reikalavimai taikomi visoms valstybinės archyvų sistemos įstaigų TIS.

27. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba įvykus esminiams pokyčiams, kurie turi įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

_____

Žurnalinių įrašų valdymo
tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

ŽURNALINIŲ ĮRAŠŲ VALDYMO TVARKOS APRAŠO PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	Statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Žurnalinių įrašų valdymo tvarkos aprašo
2 priedas

(Žurnalinių įrašų valdymo matricos forma)

ŽURNALINIŲ ĮRAŠŲ VALDYMO MATRICA

Nr.	Tinklų ir informacinės sistemos, kuriose renkami žurnaliniai įrašai	Žurnalinių įrašų rinkimo būdas	Žurnaliniai įrašai (įvykiai/ veiksmai)	Žurnaliniuose įrašuose fiksuojami duomenys	Žurnalinių įrašų analizavimo būdas (rankinis/ automatizuotas)	Žurnalinių įrašų analizavimo periodiškumas	Už žurnalinių įrašų analizavimą atsakingas SOC grupės darbuotojas	Žurnalinių įrašų analizės apibendrintos ataskaitos formavimo periodiškumas	Žurnalinių įrašų saugojimo vieta	Žurnalinių įrašų apsaugos priemonės	Žurnalinių įrašų saugojimo trukmė

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

TINKLŲ IR INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų veiklos tęstinumo valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) kritinių veiklų metu naudojamų tinklų ir informacinių sistemų (toliau – TIS) veiklos tęstinumo užtikrinimą ir jų atstatymą, įvykus kibernetiniam incidentui ar TIS sutrikimui.

2. Aprašo tikslas – suplanuoti ir įgyvendinti prevencines priemones, siekiant užkirsti kelią kibernetiniams incidentams ir TIS sutrikimams bei per trumpiausią įmanomą laikotarpį užtikrinti valstybinės archyvų sistemos įstaigų kritinių veiklų metu naudojamų TIS atkūrimą įvykus kibernetiniam incidentui ar TIS sutrikimui. Aprašo tikslas įgyvendinamas:

2.1. numatant organizacinę ir funkcinę struktūrą veiklos tęstinumui užtikrinti;

2.2. suplanuojant ir įgyvendinant prevencines priemones, siekiant užkirsti kelią kibernetiniams incidentams ar TIS sutrikimui;

2.3. suplanuojant ir įgyvendinant pasirengimo veiksmus kritinių veiklų metu naudojamų TIS atkūrimui įvykus kibernetiniam incidentui ar TIS sutrikimui;

2.4. suplanuojant finansinius, žmogiškuosius ir techninius išteklius kritinių veiklų metu naudojamų TIS atkūrimui įvykus kibernetiniam incidentui ar TIS sutrikimui;

2.5. suplanuojant veiksmus organizacijos kritinių veiklų metu naudojamoms TIS atkurti įvykus kibernetiniam incidentui ar TIS sutrikimui;

2.6. užtikrinant operatyvų sprendimų priėmimo procesą kibernetinių incidentų metu;

2.7. užtikrinant kuo mažesnius praradimus kibernetinio incidento ar TIS sutrikimo atveju.

3. Šiame Apraše vartojamos sąvokos:

3.1. **Atkūrimo laiko tikslas** (angl. *Recovery Time Objective)* (toliau – RTO) – maksimalus laikas, per kurį būtina atkurti kritinių veiklų metu naudojamą TIS po sutrikimo, kad būtų išvengta reikšmingų nuostolių;

3.2. **Atkūrimo taško tikslas** (angl. *Recovery Point Objective)* (toliau – RPO) – maksimalus priimtinas duomenų praradimo laikotarpis, skaičiuojamas nuo paskutinės galiojančios duomenų kopijos iki kibernetinio incidento ar TIS sutrikimo;

3.3. **Kritinė veikla** – veikla, kuriai sutrikus valstybinės archyvų sistemos įstaigos negali pasiekti savo strateginių tikslų;

3.4. **Maksimalus duomenų praradimo kiekis** *(angl. Maximum Tolerable Data Loss – MTDL)* (toliau – MTDL) – duomenų kiekis, kurį valstybinės archyvų sistemos

įstaigos yra pasirengusi prarasti sutrikus kritinės veiklos metu naudojamai TIS (išreiškiamas valandomis);

3.5. **Maksimalus priimtinas neveikimo laikas** (angl. *Maximum Acceptable Outage* arba *Maximum Tolerable Period of Disruption*) (toliau – MTPD) – tai maksimalus laiko intervalas, kurio metu valstybinės archyvų sistemos įstaigos gali toleruoti kritinių veiklų ir jų metu naudojamos TIS sutrikimus, kol jie dar nesukelia nepriimtinų pasekmių jos veiklai, finansinei būklei ir (ar) reputacijai;

3.6. **Poveikio veiklai vertinimas** (angl. *Business Impact Analysis*) – tai procesas, kurio metu nustatomos valstybinės archyvų sistemos įstaigų veiklos metu naudojamų TIS kritiškumas ir įvertinamas galimas finansinis, operacinis, reputacinis ir kitoks poveikis, jei šie veiklos procesai ir jų metu naudojamos TIS būtų sutrikdytos;

3.7. **Proceso savininkas** – už valstybinės archyvų sistemos įstaigos proceso (paslaugos) valdymą atsakingas darbuotojas;

3.8. **Tinklų ir informacinė sistema** – Turto valdymo apraše numatytas elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

3.9. **Tinklų ir informacinių sistemų atkūrimo kriterijai** – valstybinės archyvų sistemos įstaigų atsakingų darbuotojų nustatyti TIS veiklos kriterijai, pagal kuriuos galima nustatyti, ar TIS veikla yra atkurta;

3.10. **Veiklos atkūrimo grupė** – Lietuvos vyriausiojo archyvaro įsakymu sudaryta valstybinės archyvų sistemos įstaigų darbuotojų grupė, įgaliota užtikrinti TIS atkūrimą ir veikimą įvykus kibernetiniam incidentui ar TIS sutrikimui;

3.11. **Veiklos tęstinumo strategija** *(angl. Business continuity management strategy – BCMS)* – veiksmų ir priemonių visuma, skirta užkirsti kelią kritinės veiklos (paslaugos) sutrikimams ar sumažinti jų poveikį*;*

3.12. **Veiklos tęstinumo valdymo grupė** – Lietuvos vyriausiojo archyvaro įsakymu sudaryta valstybinės archyvų sistemos įstaigų darbuotojų grupė, įgaliota užtikrinti veiklos tęstinumui kylančių grėsmių valdymą ir veiklų atkūrimo koordinavimą įvykus kibernetiniam incidentui ar TIS sutrikimui;

3.13. **Veiklos tęstinumo valdymo planas** (toliau – VTVP) – veiksmų sąrašas, skirtas kibernetiniams incidentams ar TIS sutrikimams suvaldyti, apimantis prevencines priemones, pasirengimo priemones ir veiksmų seką kibernetinių incidentų ar TIS sutrikimų metu.

4. Aprašas parengtas vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymo ir jo įgyvendinamųjų teisės aktų reikalavimais.

5. Aprašas privalomas visiems valstybinės archyvų sistemos įstaigų darbuotojams, o pagal poreikį – ir paslaugų teikėjams ar tiekimo grandinės dalyviams.

II SKYRIUS
VEIKLOS TĘSTINUMO VALDYMO IR ATKŪRIMO PRINCIPAI

6. Veiklos tęstinumo valdymo ir atkūrimo principai:

6.1.veiklos atkūrimas – kritinių veiklų metu naudojamos TIS atkuriamos pagal valstybinės archyvų sistemos įstaigų veiklos prioritetus, nustatomus veiklos poveikio vertinimo metu. Įvykus kibernetiniam incidentui ar TIS sutrikimui veiklos tęstinumo valdymo grupė gali patikslinti veiklos prioritetus;

6.2.darbuotojų mokymas – darbuotojai turi būti supažindinti su Aprašu ir kitais valstybinės archyvų sistemos įstaigos veiklos tęstinumą reglamentuojančiais vidaus teisės aktais.

7. VTVP veiksmingumas turi būti išbandomas kiekvienais metais. Veiklos tęstinumo valdymo grupės vadovas arba jo paskirtas darbuotojas reguliariai atlieka VTVP išbandymus ir rastų trūkumų bei išmoktų pamokų pagrindu koreguoja VTVP.

8. Pagrindinis veiklos atkūrimo principas – veiklų, turinčių didžiausią neigiamą įtaką strateginiams valstybinės archyvų sistemos įstaigų tikslams įgyvendinti, metu naudojamų TIS atkūrimo pirmumas.

III SKYRIUS
ORGANIZACINĖS NUOSTATOS

9. Valstybinės archyvų sistemos įstaigų kritinių veiklų metu naudojamų TIS tęstinumui užtikrinti ir jiems atkurti sudaroma Veiklos tęstinumo valdymo grupė (toliau – VTVG) ir Veiklos atkūrimo grupė (toliau – VAG).

10. VTVG ir VAG yra sudaromos Lietuvos vyriausiojo archyvaro įsakymu, nustatant jų nariams pavestas funkcijas.

11. Į VTVG turi būti deleguojami LVAT skyrių vedėjai, kibernetinio saugumo vadovas, duomenų apsaugos pareigūnas, viešųjų ryšių atstovas ir už TIS atkūrimą atsakingas darbuotojas arba jo vadovas, valstybės archyvų direktoriai ar jų deleguoti asmenys, pagal poreikį – kiti valstybinės archyvų sistemos įstaigų darbuotojai.

12. VTVG yra atskaitinga Lietuvos vyriausiajam archyvarui.

13. VAG yra atskaitinga VTVG.

14. VTVG ir VAG nariai turi turėti reikiamas kompetencijas jiems numatytoms funkcijoms vykdyti. Šių grupių kompetencijos turi būti tobulinamos pagal poreikį organizuojant specializuotus mokymus rizikų vertinimo ir valdymo bei veiklos tęstinumo valdymo srityse ir organizuojant informavimo programas.

15. Kibernetinio saugumo vadovas, suderinęs su valstybės archyvų direktoriais, teikia Lietuvos vyriausiajam archyvarui tvirtinti Veiklos tęstinumo valdymo grupės ir atkūrimo grupės sudėtį (4 priedas).

16. VTVG vadovo funkcijos ir įgaliojimai:

16.1. organizuoja VTVG darbą ir veda jos posėdžius;

16.2. organizuoja ir koordinuoja VTVP plano parengimą ir pateikimą tvirtinti Lietuvos vyriausiajam archyvarui, užtikrina VTVP plano peržiūrą ir atnaujinimą šio Aprašo nustatytu periodiškumu;

16.3. priima sprendimą aktyvuoti VTVP;

16.4. paveda VTVG nariams vykdyti VTVP numatytas veiklas, užtikrina koordinavimą ir įgyvendinimo kontrolę;

16.5. paveda VAG atlikti Veiklos atkūrimo veiksmų plane (toliau – VAVP) numatytas veiklas, koordinuoja šias veiklas ir užtikrina jų įgyvendinimo kontrolę;

16.6. proceso savininkui pritarus, priima sprendimą grįžti prie įprastos veiklos būdo;

16.7. šio Aprašo nustatytu periodiškumu organizuoja VTVP išbandymus;

16.8. rengia ir Lietuvos vyriausiajam archyvarui teikia tvirtinti VTVP išbandymo ataskaitą.

17. VTVG funkcijos ir įgaliojimai:

17.1. rengia VTVP (gali būti bendradarbiaujama su VAG);

17.2. analizuoja kibernetinio incidento ar TIS sutrikimo priežastis, pasekmes bei šių priežasčių šalinimo būdus bei suteikia pagalbą VTVG vadovui įgyvendinant VTVP veiklas ir priimant sprendimą aktyvuoti VTVP, taip pat priimant kitus sprendimus veiklos tęstinumo valdymo klausimais;

17.3. bendrauja ir bendradarbiauja su valstybinės archyvų sistemos įstaigos kritinių veiklų metu naudojamų TIS savininkais ir naudotojais;

17.4. bendrauja ir bendradarbiauja su teisėsaugos ir kitomis institucijomis, kitomis interesų grupėmis;

17.5. planuoja finansinius ir kitus išteklius kritinių veiklų metu naudojamoms TIS atkurti įvykus kibernetiniam incidentui ar TIS sutrikimui, užtikrina jų pakankamumo ir prieinamumo kontrolę;

17.6. planuoja ir įgyvendina organizacijos prevencines priemones, leidžiančias užkirsti kelią kibernetiniams incidentams ar TIS sutrikimams;

17.7. planuoja ir įgyvendina valstybinės archyvų sistemos įstaigų pasirengimo atkurti kritinių veiklų metu naudojamas TIS veiksmus;

17.8. organizuoja duomenų ir įrangos fizinę saugą įvykus incidentui ar TIS sutrikimui;

17.9. organizuoja logistiką (žmonių, daiktų, įrangos gabenimą);

17.10. prireikus inicijuoja prekių, paslaugų, darbų, reikalingų veiklai atkurti, įsigijimą;

17.11. koordinuoja ir kontroliuoja VAG veiklą;

17.12. vykdo kitas VTVG pavestas funkcijas, susijusias su veiklos tęstinumui kylančių grėsmių valdymu ir veiklų atkūrimo koordinavimu įvykus incidentui ar TIS sutrikimui.

18. VAG vadovo funkcijos ir įgaliojimai:

18.1. organizuoja VAG darbą ir veda jos posėdžius;

18.2. paveda VAG nariams atlikti VTVP numatytas veiklas, koordinuoja šias veiklas ir užtikrina jų įgyvendinimo kontrolę;

18.3. bendradarbiauja su procesų savininkais, norint nustatyti, ar yra pasiekti VTVP nustatyti MTPD ir MTDL;

18.4. įsitikina, kad pasiekti TIS atkūrimo kriterijai.

19. VAG funkcijos ir įgaliojimai:

19.1. padeda VTVG rengti VTVP;

19.2. organizuoja, įgyvendina ir koordinuoja TIS atkūrimą įvykus kibernetiniam incidentui ar TIS sutrikimui, įskaitant, tačiau neapsiribojant:

19.2.1. tarnybinių stočių (įskaitant virtualius resursus) veiklos atkūrimą;

19.2.2. kompiuterių tinklo veikimo atkūrimą;

19.2.3. duomenų atkūrimą;

19.2.4. taikomosios programinės įrangos veikimo atkūrimą;

19.2.5. kompiuterizuotų darbo vietų veikimo atkūrimą ir prijungimą prie kompiuterių tinklo;

19.3. vykdo VTVG nurodytus veiksmus pagal VTVP;

19.4. vykdo kitas funkcijas, susijusias su TIS atkūrimu įvykus kibernetiniam incidentui ar TIS sutrikimui.

20. Už veiklos tęstinumo valdymo dokumentų parengimą atsakingas VTVG vadovas.

21. Veiklos tęstinumo valdymo dokumentus sudaro:

21.1. Lietuvos vyriausiojo archyvaro įsakymai dėl VTVG ir VGA sudarymo;

21.2. VTVG ir VAG narių kontaktinė informacija (mobiliojo telefono numeris, el. pašto adresas);

21.3. veiklos tęstinumo valdyme ir atkūrime dalyvaujančių organizacijos darbuotojų sąrašas (pareigos, vardas ir pavardė) ir jų kontaktinė informacija (mobiliojo telefono numeris, el. pašto adresas);

21.4. VTVP, parengtas pagal šio Aprašo 2 priede pateiktą Veiklos tęstinumo valdymo plano formą ir patvirtintas Lietuvos vyriausiojo archyvaro įsakymu;

21.5. Valstybinės archyvų sistemos įstaigų veiklos tęstinumo valdyme ir atkūrime dalyvaujančių paslaugų teikėjų bei tiekimo grandinės dalyvių ir jų atsakingų darbuotojų sąrašas su kontaktine informacija, sutarčių su paslaugų teikėjais sąrašas ir jų kopijos;

21.6. kritinių veiklų metu naudojamų TIS atstatymui reikalingos informacijos ir dokumentų (pvz. tinklo schemos, serverinės ar duomenų centro įrangos ir jų parametrų sąrašas ir pan.) kopijos;

21.7. kita valstybinės archyvų sistemos įstaigų veiklos tęstinumui užtikrinti ir atkurti svarbi informacija.

22. Veiklos tęstinumo valdymo dokumentai turi būti saugomi elektronine forma ir popierine forma. Jie turi būti lengvai pasiekiama VTVG ir VAG vadovams bei VTVG ir VAG grupės.

23. VTVG vadovas arba kitas jo paskirtas darbuotojas turi koordinuoti kasmetinį veiklos tęstinumo valdymo dokumentų atnaujinimą, ypač atlikus kasmetinį poveikio veiklai vertinimą ir tinklų ir informacinių sistemų rizikos vertinimą.

IV SKYRIUS
VEIKLOS TĘSTINUMO IR ATKŪRIMO PRIORITETŲ IR EILIŠKUMO NUSTATYMAS

24. Veiklos tęstinumui turinčių įtaką TIS atkūrimo prioritetai ir eiliškumas nustatomi atliekant poveikio veiklai vertinimą (toliau – Vertinimas). Vertinimo metu:

24.1. apibrėžiami poveikio vertinimo tipai (pvz. poveikis finansams, procesams, reputacijai ir pan.) ir jų kriterijai, susiję su valstybinės archyvų sistemos įstaigų kontekstu;

24.2. nustatomos valstybinės archyvų sistemos įstaigų kritinės veiklos (paslaugos) ir jų savininkai (procesų savininkai), taip pat kritinių veiklų metu naudojamos pagrindinės TIS (pvz. TIS ar jų komponentai – pvz. aparatinė ir (ar) programinė įranga, duomenų bazės ir pan.) ir jų savininkai;

24.3. pagal kiekvieną kritinę veiklą nustatomas jos MTPD;

24.4. nustatomas kiekvienos kritinės veiklos metu naudojamų visų TIS bendras atkūrimo laiko tikslas – RTO bei TIS atkūrimo kriterijai;

24.5. pagal kiekvieną kritinę veiklą nustatomas jos MTDL;

24.6. nustatomas kritinės veiklos metu naudojamos kiekvienos TIS RPO;

24.7. identifikuojama, kokių išteklių reikia kritinių veiklų metu naudojamoms TIS atkurti pagal šių procesų savininkų nustatytus MTPD laikus;

24.8. remiantis šio Aprašo IV skyriaus atlikto vertinimo metu rezultatais nustatomas kritinių veiklų metu naudojamų TIS atstatymo eiliškumas. Kuo kritinės veiklos MTPD laikas yra mažesnis, tuo jo metu naudojamos TIS turi būti atstatytos pirmiau nei kitos kitų kritinių veiklų metu naudojamos TIS.

25. Atliekant rizikos vertinimą papildomai pagal kiekvieną kritinę veiklą ir jos metu naudojamas TIS turi būti identifikuojami ir įvertinami kibernetinių incidentų ar TIS sutrikimų scenarijai (grėsmės), kuriems įvykus gali būti sutrikdytos kritinių veiklų metu naudojamos TIS.

V SKYRIUS
VEIKLOS TĘSTINUMO VALDYMO PLANO RENGIMO NUOSTATOS

26. Remiantis poveikio vertinimo ir rizikos vertinimo rezultatais, rengiamas VTVP. VTVP turi būti numatyta veiklos tęstinumo strategija ir jo įgyvendinimo veiksmų planas, t. y., prevencinės priemonės, leidžiančios užkirsti kelią kibernetiniams incidentams ar TIS sutrikimams, taip pat pasirengimo atkurti kritinių veiklų metu naudojamas TIS. VTVP taip pat turi būti numatyti detalūs kritinių veiklų metu naudojamų TIS atkūrimo veiksmai, kurie turi būti įgyvendinami per kuo trumpesnį laiką, atsižvelgiant į TIS tvarkomų duomenų tipą ir priskirtus TIS ir jo komponentų RTO laikus bei atkūrimo taško tikslus – RPO, taip pat jų aktyvavimo kriterijai.

27. VTVP rengimo metu siekiamos ir esamos situacijos įvertinimui gali būti atliktas trūkumų (neatitikčių) tarp esamos situacijos ir siekiamos situacijos vertinimas (angl. *gap analysis)*, kurio pagrindu gali būti rengiamas trūkumų (neatitikčių) šalinimo veiksmų planas.

28. VTVG parengtas ir su procesų ir TIS savininkais (pagal poreikį su kitais padalinių vadovais) suderintas VTVP projektas teikiamas tvirtinti Lietuvos vyriausiajam archyvarui.

29. Rengdama VTVP VTVG privalo užtikrinti, kad kritinių veiklų (paslaugų) tęstinumui būtinų TIS prieinamumas būtų ne mažesnis kaip 99 proc. Laiko, o svarbiausių

TIS įranga, duomenų perdavimo tinklo mazgai ir ryšio linijos būtų dubliuoti ir jų techninė būklė būtų nuolat stebima.

30. VTVG gali rengti vieną VTVP visų kritinių veiklų tęstinumui užtikrinti ir jų metu naudojamoms TIS atstatyti. Tokiu atveju VTVP turi būti detalizuoti visų TIS, naudojamų organizacijos kritinių veiklų metu, atkūrimo veiksmai, jų aktyvavimo kriterijai pagal kiekvieną rizikos vertinimo metu identifikuotą ir įvertintą kibernetinio incidento scenarijų (grėsmę). Procesų savininkams pageidaujant, VTVG pagal kiekvieną kritinę veiklą ir jos metu naudojamas TIS ar pagal kiekvieną kritinės veiklos metu naudojamą TIS turi parengti atskirus VTVP (planus).

31. VTVP turi būti peržiūrimas VTVG vadovo, dokumentuojant peržiūros faktą ir rezultatus, ne rečiau kaip kartą per metus arba po VTVP išbandymų, poveikio veiklai vertinimo ir (ar) rizikos vertinimo ir prireikus atnaujinamas.

VI SKYRIUS
VEIKLOS TĘSTINUMO VALDYMO PLANO ĮGYVENDINIMAS IR AKTYVAVIMAS

32. VTVP numatyta veiklos tęstinumo strategija ir įgyvendinimo veiklos, t. y., prevencinės priemonės, leidžiančios užkirsti kelią kibernetiniams incidentams ar TIS sutrikimams, įgyvendinamos nuolat arba VTVP numatytu dažnumu ir terminais.

33. Kibernetiniai incidentai ar TIS sutrikimai aptinkami stebėsenos įrankiais, jie registruojami ir valdomi vadovaujantis Kibernetinių incidentų valdymo plano nuostatomis. Įvykus kibernetiniam incidentui ar TIS sutrikimui, jį pastebėjęs ar nustatęs valstybinės archyvų sistemos įstaigos darbuotojas apie tai nedelsdamas turi informuoti kibernetinio saugumo vadovą. Įvykus didelio poveikio kibernetiniam incidentui, kibernetinio saugumo vadovas turi informuoti VTVG vadovą ir Nacionalinį kibernetinio saugumo centrą prie Krašto apsaugos ministerijos (toliau – NKSC) Kibernetinių incidentų valdymo plane numatytais terminais ir kanalais.

34. Kibernetinio saugumo vadovas, įtaręs neteisėtą veiklą, pažeidžiančią valstybinės archyvų sistemos įstaigos vidaus teisės aktus, reglamentuojančius kibernetinio saugumo valdymą, privalo imtis reikiamų priemonių, kad nebūtų pažeistas kibernetinis saugumas, bei apie tai privalo pranešti Lietuvos vyriausiajam archyvarui ir, jei pažeidimas įvyko/vyksta valstybės archyve, šio archyvo direktoriui.

35. TIS administratorius kibernetinio saugumo vadovą turi informuoti apie pastebėtus TIS veiklos sutrikimus, neveikiančias ar netinkamai veikiančias duomenų saugos užtikrinimo priemones, dalyvauti šalinant TIS veiklos sutrikimus.

36. TIS naudotojai, pastebėję TIS veiklos sutrikimus, neveikiančias ar netinkamai veikiančias kibernetinio saugumo priemones, nedelsiant turi apie tai pranešti TIS administratoriams ir kibernetinio saugumo vadovui.

37. Kibernetinio incidento tyrimo ir valdymo metu VTVG nariai bendrauja tarpusavyje ir su kitais kibernetinio incidento tyrime ir valdyme dalyvaujančiais valstybinės archyvų sistemos įstaigų padaliniais ir darbuotojais telefonais arba elektroniniu paštu.

38. Prireikus VTVG rengia bendrus susirinkimus su kibernetinio incidento tyrime ir valdyme dalyvaujančiais padaliniais ir darbuotojais.

39. Įvykus kibernetiniam incidentui ar TIS sutrikimui, VTVG vadovas telefonu informuoja Lietuvos vyriausiąjį archyvarą ir, jei pažeidimas įvyko/vyksta valstybės archyve, šio archyvo direktorių. Periodiškai atnaujina informaciją apie tai, kaip atkuriamos valstybinės archyvų sistemos įstaigų kritinių veiklų metu naudojamos TIS.

40. VTVP yra aktyvuojamas VTVG vadovo sprendimu įvykus didelio poveikio kibernetiniam incidentui ar TIS sutrikimui, dėl kurio sutriko valstybinės archyvų sistemos įstaigos kritinės veiklos metu naudojama TIS. VTVG vadovas kartu su valstybinės archyvų sistemos įstaigos vadovu įvertina didelio poveikio kibernetinio incidento ar TIS sutrikimo pobūdį bei mastą ir priima sprendimą aktyvuoti VTVP pagal jame numatytą konkretų arba panašų scenarijų (grėsmę), remdamiesi VTVP numatytais aktyvavimo kriterijais. Esant sudėtingiems atvejams VTVG vadovas gali organizuoti VTVG pasitarimą ir jo metu kartu su kitais VTVG nariais įvertinti didelio poveikio kibernetinio incidento ar TIS sutrikimo pobūdį bei mastą ir kolegialiai priimti sprendimą aktyvuoti VTVP. Už konkretaus valstybės archyvo TIS atkūrimo veiksmų įgyvendinimą tiesiogiai atsako to archyvo direktorius.

41. Didelio poveikio kibernetinio incidento ar TIS sutrikimo metu šalinant incidento padarinius, siekiant atkurti kritinių veiklų naudojamas TIS, prireikus gali būti naudojamos atsarginės patalpos, kurios turi atitikti šiuos minimaliuosius reikalavimus:

41.1. būti fiziškai apsaugotos nuo neteisėto patekimo į jas – patalpos turi būti rakinamos;

41.2. turėti nuolatinį elektros energijos šaltinį ir interneto ryšį, taip pat ryšį su valstybinės archyvų sistemos įstaigos kompiuterių tinklu;

41.3. atitikti gaisrinės saugos ir higienos reikalavimus, jose turi būti veikianti oro vėdinimo ir kondicionavimo įranga.

42. Sprendimą sugrįžti į įprastas veiklos sąlygas ir sustabdyti VTVP priima VTVG vadovas, suderinęs su konkrečios valstybinės archyvų sistemos įstaigos vadovu, kai yra pašalintos visos pagrindinės didelio poveikio kibernetinio incidento ir (ar) TIS sutrikimo atsiradimo priežastys, atstatytos visos įstaigos kritinių veiklų metu naudojamos TIS (pasiekti TIS atkūrimo kriterijai) bei atlikti po atkūrimo veiksmai pagal VTVP. VTVG vadovas, priimdamas sprendimą sustabdyti VTVP, turi konsultuotis su atitinkamos valstybinės archyvų sistemos įstaigos atstatomų TIS ir procesų savininkais. Apie priimtą sprendimą sustabdyti VTVP VTVG vadovas, suderinęs su konkretaus valstybės archyvo vadovu, informuoja Lietuvos vyriausiąjį archyvarą, VTVG ir VAG narius bei atitinkamos įstaigos darbuotojus. Kitas suinteresuotąsias šalis apie priimtą sprendimą VTVG vadovas informuoja pagal poreikį.

VII SKYRIUS
VEIKLOS TĘSTINUMO VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

43. Siekiant užtikrinti VTVP veiksmingumą, ne rečiau kaip kartą per metus atliekamas VTVP išbandymas.

44. VTVP išbandymus organizuoja VTVG vadovas arba jo pavedimu kitas VTVG narys. VTVP išbandymai atliekami pagal VTVG ir (ar) VAG narių ir (ar) kibernetinio saugumo vadovo sukurtą kibernetinio incidento ar TIS sutrikimo scenarijų.

45. VTVP pagal sukurtą kibernetinio incidento ar TIS sutrikimo scenarijų VTVG ir VAG išbando kartu.

46. Už VTVP išbandymo plano parengimą pagal šio Aprašo 3 priede numatytą Veiklos tęstinumo valdymo plano veiksmingumo išbandymo plano formą, VTVP išbandymų organizavimą, VTVP išbandymų ataskaitos pagal šio Aprašo 4 priede numatytą Veiklos tęstinumo valdymo plano veiksmingumo išbandymo ataskaitos formą ir VTVP išbandymų metu nustatytų trūkumų šalinimo plano parengimą ir pateikimą Lietuvos vyriausiajam archyvarui atsakingas VTVG vadovas.

47. VTVG vadovas arba jo pavedimu kitas VTVG narys VTVP išbandymų metu parengia VTVP išbandymų ataskaitą (toliau – Ataskaita), kurioje fiksuojama VTVP išbandymo eiga, rezultatai, pastebėti VTVP trūkumai ir visų VTVP išbandymo dalyvių pastabos. Ataskaitoje turi būti nurodyta VTVP išbandymo data, eiga ir rezultatai, išbandymo metu pastebėti trūkumai, jų pašalinimo svarba ir laikas, per kurį trūkumai turi būti pašalinti.

48. Lietuvos vyriausiasis archyvaras per 5 darbo dienas nuo Ataskaitos pateikimo dienos turi ją patvirtinti ir pateikti valstybinės archyvų sistemos įstaigos atsakingiems darbuotojams.

49. Kibernetinio saugumo vadovas Ataskaitą Kibernetinio saugumo įstatymo nustatyta tvarka per 5 darbo dienas turi pateikti į NKSC administruojamą Kibernetinio saugumo informacinę sistemą.

50. VTVP išbandymo metu pastebėtų trūkumų šalinimo principai:

50.1. pastebėti trūkumai per 5 darbo dienas nuo VTVP išbandymo atlikimo dienos aptariami VTVG prieš parengiant ataskaitą;

50.2. pastebėti trūkumai fiksuojami Ataskaitoje;

50.3. bendro VTVG susitikimo metu nustatomi pastebėtų trūkumų šalinimo prioritetai, numatomos reikiamos lėšos šiems trūkumams pašalinti, laikas, per kurį trūkumai privalo būti pašalinti, ir už tai atsakingi asmenys;

50.4. pašalinus visus trūkumus ir pakoregavus VTVP, per 3 mėnesius nuo pakoreguoto VTVP patvirtinimo dienos turi būti surengti pakartotiniai VTVP išbandymai;

50.5. pakartotiniai VTVP išbandymai turi būti vykdomi ta pačia tvarka, kaip ir pradiniai VTVP išbandymai (išbandoma ir ta VTVP dalis, kurioje trūkumų neaptikta).

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

51. Visi valstybinės archyvų sistemos įstaigos valdomų TIS darbuotojai privalo laikytis šio Aprašo.

52. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba kai įvyksta esminiai pokyčiai valstybinės archyvų sistemos įstaigose, kurie turi įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

Veiklos tęstinumo valdymo
tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

VEIKLOS TĘSTINUMO VALDYMO TVARKOS APRAŠO APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	Statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Veiklos tęstinumo valdymo
tvarkos aprašo
2 priedas

(Veiklos tęstinumo valdymo plano forma)

VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. Veiklos tęstinumo valdymo plano rengimo duomenys

1 lentelė. Veiklos tęstinumo valdymo plano rengimo duomenys:

Eil. Nr.	Planą parengusio darbuotojo vardas ir pavardė	Pareigos	Parengimo / atnaujinimo data	Versija	Patvirtinimo data	Registracijos numeris

II. Kritinė veikla (paslauga) ir jos metu naudojamos TIS bei jų pagrindinės atkūrimo charakteristikos

2 lentelė. Kritinė veikla (paslauga) ir jos metu naudojamos TIS bei jų savininkai (įrašoma informacija, gauta atlikus Aprašo 24.2 punkte numatytą veiklą):

Eil. Nr.	Kritinės veiklos (paslaugos) pavadinimas	Proceso savininko pareigos, vardas ir pavardė	Kritinės veiklos (paslaugos) metu naudojamos TIS pavadinimas	TIS savininko pareigos, vardas ir pavardė
1.				

3 lentelė. Kritinės veiklos (paslauga) ir jos metu naudojamų TIS atstatymo rodikliai:

Eil. Nr.	Kritinės veiklos (paslaugos) pavadinimas	Proceso savininko pareigos, vardas ir pavardė	Didžiausias toleruotinas sutrikimo laikotarpis (MTPD)	Atkūrimo laiko tikslas (RTO)	Maksimalus duomenų praradimo kiekis (MTDL)	Atkūrimo laiko taškas (RPO)
1.	*Įrašoma informacija, gauta atlikus Aprašo 24.2 punkte numatytą veiklą*	*Įrašoma informacija, gauta atlikus Aprašo 24.2 punkte numatytą veiklą*	*Įrašoma informacija, gauta atlikus Aprašo 24.3 punkto numatytą veiklą*	*Įrašoma informacija, gauta atlikus Aprašo 24.4 punkte numatytą veiklą*	*Įrašoma informacija, gauta atlikus Aprašo 24.5 punkto numatytą veiklą*	*Įrašoma informacija, gauta atlikus Aprašo 24.6 punkto numatytą veiklą*

III. Kibernetinių incidentų sąrašas ir jų vertinimas

4 lentelė. Kibernetinių incidentų ar TIS sutrikimo scenarijų sąrašas ir jų vertinimas.

Eil. Nr.	**Incidento ar sutrikimo scenarijaus pavadinimas ir trumpas aprašymas**	**Incidento ar sutrikimo tikimybė (nuo 1 iki 5, kai 1 mažai tikėtina ir 5 labai tikėtina)**	**Incidento ar sutrikimo poveikis (nuo 1 iki 5, kai 1 mažas poveikis ir 5 labai didelis poveikis)**	**Incidento ar sutrikimo rizikos lygis**	**Rizikos priimtinumo vertinimas**	**Sprendimas, ar rengiamas Veiklos tęstinumo valdymo planas**
(1)	*(2)*	*(3)*	*(4)*	*(3*4=5)*	*(6)*	*(7)*
1.	*Įrašoma informacija, gauta atlikus Aprašo 25 punkto numatytą veiklą*	*Įrašoma informacija, gauta atlikus Aprašo 25 punkto numatytą veiklą*	*Įrašoma informacija, gauta atlikus Aprašo 25 punkto numatytą veiklą*	*Įrašoma informacija, gauta atlikus Aprašo 25 punkte numatytą veiklą*	Rizika priimtina / nepriimtina	Rengiamas / nerengiamas

IV. Veiklos tęstinumo strategija ir jo įgyvendinimo veiksmų planas

5 lentelė. Veiklos tęstinumo strategija ir jos įgyvendinimo veiksmų planas (įrašoma informacija, gauta atlikus Aprašo 26 punkte numatytą veiklą):

Eil. Nr.	**Veiklos tęstinumo strategijos pavadinimas ir trumpas aprašymas**	**Veiklos tęstinumo strategijos įgyvendinimo veiklos pavadinimas**	**Atsakingo padalinio vadovo ir (ar) darbuotojo pareigos, vardas ir pavardė**	**Įgyvendinimo dažnumas / terminai (iki)**
1.				

6 lentelė. Trūkumų (neatitikčių) šalinimo plano veiksmai*(įrašoma informacija, gauta atlikus Aprašo 27 punkte numatytą veiklą):

Eil. Nr.	**Incidento scenarijaus pavadinimas**	**Neatitikties aprašymas**	**Veiklos pavadinimas**	**Įgyvendinimo terminas (iki)**	**Atsakingo padalinio vadovo ir (ar) darbuotojo pareigos, vardas ir pavardė**
1.					

**Siekiamos ir esamos situacijos įvertinimui gali būti atliktas trūkumų (neatitikčių) vertinimas (angl. gap analysis), kurio pagrindu parengiamas trūkumų (neatitikčių) šalinimo veiksmų planas.*

Kritinę veiklą (paslaugą) ir jos metu naudojamas TIS reglamentuojantys dokumentai: [pateikiamos nuorodos į dokumentus, pvz., nacionalinius ar vidaus teisės aktus reglamentuojančius veiklą ir t.t.]

V. Atsakingų asmenų ir trečiųjų šalių kontaktai

7 lentelė. Veiklos tęstinumo valdymo grupės sudėtis:

Eil. Nr.	Vardas, pavardė	Pareigos	Vaidmuo	Kontaktai	Pavaduojantis darbuotojas	Pavaduojančio darbuotojo kontaktai

8 lentelė. Veiklos atkūrimo grupės sudėtis:

Eil. Nr.	Vardas, pavardė	Pareigos	Vaidmuo	Kontaktai	Pavaduojantis darbuotojas	Pavaduojančio darbuotojo kontaktai

9 lentelė. Pagrindiniai tiekėjų kontaktai:

Eil. Nr.	Tiekėjo pavadinimas	Veiklos sritis	Tiekėjo atsakingo darbuotojo pareigos, vardas ir pavardė	Kontaktai	Kontaktuojančio darbuotojo pareigos, vardas ir pavardė

10 lentelė. Pagrindinių klientų kontaktai:

Eil. Nr.	Kliento pavadinimas	Teikiamos paslaugos	Kliento atsakingo darbuotojo pareigos, vardas ir pavardė	Kontaktai	Kontaktuojančio darbuotojo pareigos, vardas ir pavardė

VI. Veiklos atkūrimo veiksmų planas pagal scenarijus

Scenarijus Nr. 1 (probleminės situacijos) aprašymas:[pateikiamas scenarijus, kuriam parengtas Veiklų atkūrimo veiksmų planas]

Aktyvavimo kriterijai:[nurodomos sąlygos, kada pradedamas taikyti Veiklų atkūrimo veiksmų planas]

11 lentelė. Detalieji valdymo veiksmai:

	Eil. Nr.	Veiksmas	Atsakingas asmuo	Trukmė	Bendra trukmė	Rezultatai	Papildoma informacija	Data, laikas, atlikęs darbuotojas
REAGAVIMAS	1.							
ATSTATYMAS	1.							
PO ATSTATYMO								
	1.							

TIS atkurti reikalingi dokumentai:
[pateikiamos nuorodos į dokumentus, pvz. brėžiniai, įrangos specifikacijos, tinklo fizinės ir loginės schemos ir t.t.]

Scenarijus Nr. 2 (probleminės situacijos) aprašymas:
[pateikiamas scenarijus, kuriam parengtas Veiklų atkūrimo veiksmų planas]

Aktyvavimo kriterijai:
[nurodomos sąlygos, kada pradedamas taikyti Veiklų atkūrimo veiksmų planas]

12 lentelė. Detalieji valdymo veiksmai:

	Eil. Nr.	Veiksmas	Atsakingas darbuotojas	Trukmė	Bendra trukmė	Rezultatai	Papildoma informacija	Data, laikas, atlikęs darbuotojas
REAGAVIMAS	1.							
ATSTATYMAS	1.							
PO ATSTATYMO								
	1.							

TIS atkurti reikalingi dokumentai:
[pateikiamos nuorodos į dokumentus, pvz. brėžiniai, įrangos specifikacijos, tinklo fizinės ir loginės schemos ir t.t.]

Veiklos tęstinumo valdymo
tvarkos aprašo
3 priedas

(Veiklos tęstinumo valdymo plano išbandymo forma)

VEIKLOS TĘSTINUMO VALDYMO PLANO IŠBANDYMO PLANAS

1. Veiklos tęstinumo valdymo plano išbandymo numatoma data:

_____

2. Veiklos tęstinumo valdymo plano išbandymo tikslas ir uždaviniai:

_____

_____

3. Testuojamas kibernetinio incidento scenarijus:

_____

_____

4. Veiklos tęstinumo valdymo plano išbandymo apimtis (testuojama kritinė veikla ir jos metu naudojamos TIS ir (ar) jų komponentai):

_____

_____

_____

_____

1 lentelė. Veiklos tęstinumo valdymo plano išbandymo dalyvių sąrašas:

Eil. Nr.	**Vardas ir pavardė**	**Pareigos**	**Vaidmuo**	**Kontaktai**

_____

Veiklos tęstinumo valdymo
tvarkos aprašo
4 priedas

(Veiklos tęstinumo valdymo plano veiksmingumo išbandymo ataskaitos forma)

VEIKLOS TĘSTINUMO VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO ATASKAITA

1. Veiklos tęstinumo valdymo plano išbandymo dalyviai.

1 lentelė. Veiklos tęstinumo valdymo plano išbandymo dalyvių sąrašas:

Eil. Nr.	**Vardas ir pavardė**	**Pareigos**	**Vaidmuo**	**Kontaktai**

2. Kibernetinio incidento ar TIS sutrikimo scenarijaus apibūdinimas:

3. Kritinė veiklos sritis ir jos metu naudojama TIS, kurią paveikė kibernetinis incidentas ar TIS sutrikimas:

4. Veiklos tęstinumo valdymo plano išbandymo eiga (eigos santrauka) ir trukmė:

5. Apibendrinti veiklos tęstinumo valdymo plano išbandymo rezultatai (sėkmingi, nesėkmingi):

6. Veiklos tęstinumo valdymo plano išbandymo tikslų ir uždavinių pasiekimas (pasiekta, nepasiekta, pasiekta iš dalies, nurodant, kokie buvo pasiekti, iš dalies pasiekti ar nepasiekti RTO rodikliai):

7. Nustatyti veiklos tęstinumo valdymo plano trūkumai:

8. Siūlymai keisti arba papildyti veiklos tęstinumo valdymo planą:

(vardas, pavardė) (parašas)

(vardas, pavardė)	(parašas)

Veiklos tęstinumo valdymo
tvarkos aprašo
5 priedas

(Veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės sudėties forma)

VEIKLOS TĘSTINUMO VALDYMO GRUPĖS IR VEIKLOS ATKŪRIMO GRUPĖS SUDĖTIS

1 lentelė. Veiklos tęstinumo valdymo grupės nariai:

Eil. Nr.	Vardas, pavardė	Padalinys	Pareigos	Atsakomybė	Kontaktai

2 lentelė. Veiklos atkūrimo grupės nariai:

Eil. Nr.	Vardas, pavardė	Padalinys	Pareigos	Atsakomybė	Kontaktai

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

ATSARGINIŲ DUOMENŲ KOPIJŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Atsarginių duomenų kopijų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) tinklų ir informacinių sistemų atsarginių duomenų kopijų kūrimo, saugojimo, atkūrimo ir atkūrimo testavimo tvarką.

2. Apraše vartojamos sąvokos:

2.1. **Atkūrimo objektas** – virtuali mašina (angl. *virtual machine*), visi arba pavieniai failai, duomenų bazės failas, operacinė sistema, taikomoji programinė įranga, konfigūracijos ir kt., priklausomai nuo valstybinės archyvų sistemos įstaigos tinklų ir informacinių sistemų struktūros;

2.2. **Atkūrimo tipas** – tai atsarginių kopijų atkūrimo būdas arba metodas, pvz., pilnas atkūrimas (angl. *Full restore*), dalinis atkūrimas (angl. *Granular/Partial restore*), momentinio vaizdo atkūrimas (angl. *Snapshot restore*) ir kt., taikomas siekiant atkurti pasirinktą objektą;

2.3. **Atsarginė kopija** – tinklų ir informacinių sistemų duomenų arba kitų atkūrimo objektų kopija, sukurta ir saugoma siekiant atkurti pradinę būklę duomenų praradimo, pažeidimo, techninio gedimo, kibernetinio incidento ar kitos veiklos sutrikimo atveju;

2.4. **Kritinė klaida** – klaida, dėl kurios atsarginės kopijos atkūrimo procesas tampa nesėkmingas arba dėl kuriuos tinklų ir informacinė sistema (ar jų dalis) negali būti atkurta per nustatytą atkūrimo laikotarpį;

2.5. **Maksimalus duomenų praradimo kiekis** *(angl. Maximum Tolerable Data Loss – MTDL)* (toliau – MTDL) – duomenų kiekis, kurį valstybinės archyvų sistemos įstaiga yra pasirengusi prarasti sutrikus kritinės veiklos metu naudojamai TIS (išreiškiamas valandomis);

2.6. **Maksimalus priimtinas neveikimo laikas** (angl. *Maximum Acceptable Outage* arba *Maximum Tolerable Period of Disruption*) (toliau – MTPD) – tai maksimalus laiko intervalas, kurio metu valstybinės archyvų sistemos įstaiga gali toleruoti kritinių veiklų ir jų metu naudojamos TIS sutrikimus, kol jie dar nesukelia nepriimtinų pasekmių jos veiklai, finansinei būklei ir (ar) reputacijai;

2.7. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

2.8. **Atkūrimo laiko tikslas** (angl. *Recovery Time Objective)* (toliau – RTO) – maksimalus laikas, per kurį būtina atkurti kritinių veiklų metu naudojamą TIS po sutrikimo, kad būtų išvengta reikšmingų nuostolių;

2.9. **Atkūrimo taško tikslas** (angl. *Recovery Point Objective)* (toliau – RPO) – maksimalus priimtinas duomenų praradimo laikotarpis, skaičiuojamas nuo paskutinės galiojančios duomenų kopijos iki kibernetinio incidento ar TIS sutrikimo.

3. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Lietuvos Respublikos kibernetinio saugumo įstatyme.

4. Už tinkamą atsarginių duomenų kopijų valdymo procesą yra atsakingas kibernetinio saugumo vadovas.

5. Atsargines kopijas kuria, saugo, atkuria ir atlieka kopijų atkūrimo testavimus TIS administratorius (jei paslauga perkama – šias funkcijas pagal paslaugų teikimo sutartį atlieka paslaugos teikėjas pagal Teikėjų grandinės valdymo tvarkos aprašą).

II SKYRIUS
ATSARGINIŲ DUOMENŲ KOPIJŲ KŪRIMAS

6. Atsarginių duomenų kopijų kūrimo procesas valstybinės archyvų sistemos įstaigoje vykdomas pagal tris duomenų saugojimo grupes:

6.1. už organizacijos infrastruktūroje saugomų duomenų kopijų kūrimą yra atsakingas TIS administratorius;

6.2. už duomenų centre saugomų duomenų atsarginių kopijų kūrimą (įskaitant jų inicijavimą, saugojimą ir atkūrimo testavimą) yra atsakingas paslaugos teikėjas, su kuriuo sudaryta paslaugų teikimo sutartis, o TIS administratorius privalo užtikrinti, kad paslaugų teikėjas vykdytų sutartus įsipareigojimus;

6.3. už debesijoje saugomų duomenų atsarginių kopijų kūrimą ir atkūrimą atsakomybė priskirta debesijos paslaugų teikėjui pagal paslaugų lygio sutartį (SLA), o TIS administratorius privalo reguliariai tikrinti, ar debesijos paslaugų teikėjo atliekamos procedūros atitinka šio Aprašo reikalavimus.

7. Duomenų atsarginės kopijos kuriamos automatinėmis elektroninių duomenų kopijavimo priemonėmis nustatytu periodiškumu, nustatomu vadovaujantis Tinklų ir informacinių sistemų veiklos tęstinumo valdymo tvarkoje nustatytais TIS atkūrimo reikalavimais, priklausomai nuo kopijavimo duomenų svarbos:

7.1. atsižvelgiant į TIS RPO, kurie turi būti suderinti su MTDL;

7.2. atsižvelgiant į TIS RTO, kurie turi būti suderinti su MTPD.

8. Atsarginės duomenų kopijos kuriamos TIS, jų komponentams ir juose ar su jais susijusiems duomenims.

9. TIS administratorius kartu su kibernetinio saugumo vadovu turi parengti ir patvirtinti TIS, kurioms kuriamos atsarginės duomenų kopijos, sąrašą (žr. 2 priedą).

10. Prieiga prie šio Aprašo 2 priedo turi būti suteikiama tik darbuotojams, kuriems ši informacija reikalinga tarnybos funkcijoms vykdyti.

11. Atsarginių duomenų kopijų valdymo kontrolei užtikrinti TIS administratorius turi įdiegti:

11.1. duomenų kopijų saugyklų talpos kitimo fiksavimo ir kontrolės priemones;

11.2. prieigos prie duomenų ir jų peržiūros fiksavimo ir kontrolės priemones;

11.3. klaidų fiksavimo laikmenose ir kopijų darymo įrenginiuose priemones;

11.4. informacijos apie duomenų kopijų judėjimą (perkėlimą į kitą saugyklą arba laikmeną) fiksavimo ir kontrolės priemones;

11.5. atsarginių duomenų kopijų darymo ir šių duomenų atkūrimo iš atsarginių duomenų kopijų priemones;

11.6. periodinį atsarginių duomenų kopijų kokybės ir vientisumo tikrinimą.

12. Atsižvelgiant į kopijuojamų duomenų svarbą ir apimtį, gali būti kuriamos skirtingų tipų atsarginės duomenų kopijos:

12.1. pilna atsarginė kopija (angl. *full backup*) – sukuriama visa pasirinktų duomenų ar sistemų kopija. Naudojama, kai būtina visiškai atkurti sistemą, siekiant užtikrinti veiklos tęstinumą, arba kai to reikalauja teisės aktai;

12.2. dalinė inkrementinė kopija (angl. *incremental backup*) – saugomi tik tie duomenys, kurie pasikeitė po paskutinės atsarginės kopijos (pilnos arba inkrementinės). Naudojama siekiant optimizuoti saugyklos naudojimą ir sutrumpinti kopijavimo laiką;

12.3. dalinė diferencialinė kopija (angl. *differential backup*) – saugomi visi pasikeitimai nuo paskutinės pilnos atsarginės kopijos. Naudojama kaip kompromisas tarp atkūrimo greičio ir saugyklos naudojimo.

13. Informacija apie duomenų kopijos kūrimą (kopijos įrašymo data, laikas ir kt.) automatiškai fiksuojama ir saugoma atsarginių duomenų kopijų darymo žurnale (angl. *log file*) pagal Žurnalinių įrašų valdymo tvarkos aprašą.

III SKYRIUS
ATSARGINIŲ DUOMENŲ KOPIJŲ SAUGOJIMAS

14. Atsarginės kopijos daromos ir laikomos geografiškai nutolusioje vietoje, kuri užtikrina fizinę ir logistinę atskirtį nuo pagrindinės veiklos vietos, kad būtų sumažinta rizika dėl bendrų poveikio veiksnių (pvz., gaisro, potvynio, elektros tiekimo sutrikimų ar kibernetinio incidento).

15. Atsarginės kopijos saugomos šifruotos, naudojant Kriptografijos ir šifravimo naudojimo tvarkos apraše numatytus šifravimo raktus.

16. Atsarginių duomenų kopijų saugojimo ir ištrynimo terminai apibrėžiami kiekvienai TIS, nurodytai Turto valdymo tvarkos aprašo prieduose.

17. Pasibaigus duomenų atsarginės kopijos saugojimo laikotarpiui, ji turi būti sunaikinama saugiu būdu, atsižvelgiant į informacijos klasifikaciją pagal Turto valdymo tvarkos aprašą:

17.1. konfidencialios informacijos atsarginės kopijos sunaikinamos naudojant saugaus šalinimo būdus (pvz., kriptografinį perrašymą, fizinį laikmenos sunaikinimą), fiksuojant sunaikinimo faktą;

17.2. viešos informacijos atsarginės kopijos gali būti ištrinamos įprastu automatizuotu būdu.

18. Patalpos, kuriose yra saugomos atsarginės duomenų kopijos, turi būti apsaugotos nuo neteisėto asmenų patekimo į jas, taikant fizines ar elektronines apsaugos priemones:

18.1. jei atsarginės kopijos saugomos valstybinės archyvų sistemos įstaigos infrastruktūroje, turi būti įrengtas fizinis įėjimo kontrolės mechanizmas (pvz., fizinis raktas, magnetinės kortelės, biometrinė autentifikacija), vaizdo stebėjimo priemonės, signalizacija, taip pat užtikrintas ribotas ir dokumentuotas fizinis priėjimas tik įgaliotiems asmenims bei kitos priemonės pagal Fizinės apsaugos tvarkos aprašą;

18.2. jei atsarginės kopijos saugomos paslaugų teikėjo infrastruktūroje (duomenų centre arba debesijoje), paslaugų teikėjas turi būti įsipareigojęs užtikrinti fizinį atsarginių kopijų saugumo lygį, atitinkantį ne mažesnį, nei nustatyta Fizinės apsaugos tvarkos apraše ir Tiekimo grandinės saugumo valdymo tvarkos apraše. Fizinės apsaugos priemonės ir procedūros turi būti dokumentuotos paslaugų teikimo sutartyje;

18.3. patekimas į patalpas, kuriose saugomos atsarginės duomenų kopijos, yra kontroliuojamas Fizinės apsaugos tvarkos apraše nustatyta tvarka.

IV SKYRIUS
ATSARGINIŲ DUOMENŲ KOPIJŲ ATKŪRIMAS

19. Duomenys iš atsarginių duomenų kopijų atkuriami:

19.1. įvykus informacijos saugumo incidentui, kai TIS duomenys sunaikinami, sugadinami ar pakeičiami, kai panaikinama ar apribojama galimybė naudotis duomenimis arba sutrinka TIS veikimas;

19.2. atkūrimo testavimo metu, siekiant patikrinti atsarginių kopijų atkūrimo galimybes pagal nustatytus RTO ir RPO reikalavimus.

20. Duomenų atkūrimo veiksmai iš atsarginių duomenų kopijų vykdomi Tinklų ir informacinių sistemų veiklos tęstinumo valdymo tvarkos apraše nustatyta tvarka.

21. Turi būti numatytos atsarginės patalpos, į kurias galima būtų laikinai perkelti TIS įrangą, nesant galimybių tęsti veiklos pagrindinėse patalpose. Atsarginės patalpos turi atitikti pagrindinėms patalpoms keliamus reikalavimus, nustatytus Fizinės apsaugos tvarkos apraše.

22. TIS administratorius duomenų atkūrimo metu turi patikrinti TIS atkurtų duomenų vientisumą ir prieinamumą bei suderinamumą valstybinės archyvų sistemos įstaigoje.

V SKYRIUS
ATSARGINIŲ DUOMENŲ KOPIJŲ ATKŪRIMO TESTAVIMAS

23. Turi būti naudojama speciali programinė įranga, kuri automatiškai patikrina, ar iš duomenų kopijos galima atkurti duomenis, kurie būtų visiškai funkcionalūs. Jeigu tokia programinė įranga nenaudojama, tuomet TIS administratorius iki kiekvienų metų sausio 31 d. parengia ir patvirtina Atsarginių duomenų kopijų atkūrimo testavimo kalendorinį grafiką (3 priedas) jame nurodydamas TIS, atkūrimo objektą ir jų atsarginių duomenų kopijų atkūrimo testavimo periodiškumą.

24. Atsarginių duomenų kopijų valdymo procesą valstybinės archyvų sistemos įstaigose koordinuoja ir už jo tinkamą įgyvendinimą atsako TIS administratorius, kuris pasitelkęs paslaugas teikiančias trečiąsias šalis atlieka atsarginių duomenų kopijų atkūrimo

testavimus ir pildo atsarginių duomenų kopijų atkūrimo stebėsenos formą (4 priedas), kurioje nurodo:

24.1. TIS pavadinimą;

24.2. atkūrimo objektą;

24.3. atkūrimo tipą;

24.4. atsarginės kopijos atkūrimo laiką, kurį sudaro RTO ir realus atkūrimo laikas bei jų skirtumas;

24.5. įvykusias klaidas, klaidų pavadinimą ir skaičių;

24.6. atkūrimo įgyvendinimą procentine išraiška;

24.7. pastabas ir pasiūlymus.

25. TIS administratorius, atlikęs atsarginių duomenų kopijų atkūrimo testavimą, užpildo ir pasirašo Atsarginių duomenų kopijų atkūrimo stebėsenos formą bei pateikia ją kibernetinio saugumo vadovui peržiūrėti ir tvirtinti.

26. TIS administratorius kartu su kibernetinio saugumo vadovu peržiūri atsarginių duomenų kopijų atkūrimo testavimo rezultatus ir įvertina, ar jie atitinka šiuos sėkmingo atkūrimo rodiklius:

26.1. realus atkūrimo laikas neviršija nustatyto RTO laiko;

26.2. atkūrimo metu nebuvo užfiksuota kritinių klaidų, dėl kurių galėjo sutrikti atkūrimo procesas ar dėl kurių galėjo nepavykti atkurti duomenis;

26.3. sėkmingas atkurto atkūrimo objekto procentas, leidžiantis užtikrinti minimalų atkurto atkūrimo objekto naudojimą be reikšmingų veikimo sutrikimų.

27. Atsarginių duomenų kopijų atkūrimo stebėsenos formą saugoma ne trumpiau nei 3 metus po atsarginių duomenų kopijų atkūrimo testavimų.

28. Jei atsarginių duomenų kopijų atkūrimo testavimo metu nustatoma, kad atkūrimo testavimo rezultatai neatitinka bent vieno šio Aprašo 26 punkte nustatytų sėkmingo atkūrimo rodiklių, priežastys turi būti šalinamos, įtraukiant priemones į Rizikų valdymo planą, rengiamą pagal Tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarkos aprašą.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

29. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba atsiradus esminių pokyčių, galinčių turėti įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

_____

Atsarginių duomenų kopijų
valdymo tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

ATSARGINIŲ DUOMENŲ KOPIJŲ VALDYMO TVARKOS PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Atsarginių duomenų kopijų
valdymo tvarkos aprašo
2 priedas

(Tinklų ir informacinių sistemų, kuriems kuriamos atsarginės duomenų kopijos, sąrašo forma)

TINKLŲ IR INFORMACINIŲ SISTEMŲ, KURIOMS KURIAMOS ATSARGINĖS DUOMENŲ KOPIJOS, SĄRAŠAS

Nr.	Tinklų ir informacinės sistemos pavadinimas	Kopijos kūrimo objektas	Kopijos kūrimo tipas	Kopijos kūrimas		Kopijos saugojimas		
				RPO (kopijos kūrimo dažnumas)	Už kopijos kūrimą atsakingo darbuotojo pareigos, vardas ir pavardė ar paslaugų teikėjo pavadinimas	Kopijos saugojimo vieta	Kopijos saugojimo terminas (dienų skaičius)	Už kopijos saugojimą atsakingo darbuotojo pareigos, vardas ir pavardė ar paslaugų teikėjo pavadinimas

_____

Atsarginių duomenų kopijų
valdymo tvarkos aprašo
3 priedas

(Atsarginių duomenų kopijų atkūrimo kalendorinio grafiko forma)

ATSARGINIŲ DUOMENŲ KOPIJŲ ATKŪRIMO TESTAVIMO KALENDORINIS GRAFIKAS

Nr.	Tinklų ir informacinės sistemos pavadinimas	Atkūrimo objektas	Kalendoriniai metai [nurodomi metai]			
			I ketvirtis/ atkūrimo tipas	II ketvirtis/ atkūrimo tipas	III ketvirtis/ atkūrimo tipas	IV ketvirtis/ atkūrimo tipas

_____

Atsarginių duomenų kopijų
valdymo tvarkos aprašo
4 priedas

(Atsarginių duomenų kopijų atkūrimo stebėsenos ataskaitos forma)

ATSARGINIŲ DUOMENŲ KOPIJŲ ATKŪRIMO STEBĖSENOS ATASKAITA

Nr.	Tinklų ir informacinės sistemos pavadinimas	Atkūrimo objektas	Atkūrimo tipas	Atkūrimo laikas (val. min.)			Įvykusios kritinės klaidos		Atkūrimo įgyvendinimas proc.	Pastabos/ pasiūlymai
				RTO (atkūrimo laikotarpis)	Realus atkūrimo laikas	Skirtumas	Klaidos pavadinimas ir jos aprašymas	Klaidų skaičius		

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

TIEKIMO GRANDINĖS SAUGUMO VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tiekimo grandinės saugumo valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybai (toliau – LVAT) ir valstybės archyvams (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) trečiųjų šalių teikiamoms paslaugoms ir (ar) produktams (įrangai), susijusiems su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra ir modernizavimu ir (ar) kibernetinio saugumo užtikrinimu, kibernetinės saugos, kokybės ir prieigos kontrolės reikalavimus.

2. Aprašas taikomas valstybinės archyvų sistemos įstaigoms bendradarbiaujant arba planuojant bendradarbiauti su trečiosiomis šalimis (pvz., vykdant bendrus projektus, sudarant sutartis, įsigyjant paslaugas ir (ar) produktus), kurių teikiamos paslaugos ir (ar) produktai yra tiesiogiai arba netiesiogiai susiję su tinklų ir informacinių sistemų projektavimu, kūrimu, diegimu, naudojimu, priežiūra, atnaujinimu ar kibernetinės saugos užtikrinimu. Aprašo tikslas – sumažinti galimas valstybinės archyvų sistemos įstaigų tinklų ir informacinių sistemų kibernetinio saugumo rizikas.

3. Apraše vartojamos sąvokos:

3.1. **„Būtina žinoti"** – minimalus informacijos kiekis, kurį būtina žinoti prekėms pateikti, darbui atlikti ar paslaugai suteikti;

3.2. **Kibernetinio saugumo vadovas** – asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

3.3. **Privalomas paslaugų teikimo lygis** (angl. *Service Level Agreement*) (toliau – SLA) – sutartinis susitarimas tarp trečiosios šalies ir valstybinės archyvų sistemos įstaigos, kuriame nustatomi konkretūs paslaugų teikimo kokybės, prieinamumo, reagavimo į incidentus, problemų sprendimo ir kiti su paslaugų teikimu susiję rodikliai;

3.4. **Sutartis** – tarp valstybinės archyvų sistemos įstaigos ir trečiosios šalies pasirašyta tinklų ir informacinių sistemų valdymo ir (ar) kibernetinės saugos užtikrinimo paslaugų ir (ar) produktų pirkimo sutartis;

3.5. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

3.6. **Trečioji šalis** – tai išorinė organizacija, asmuo ar subjektas, teikiantis valstybinės archyvų sistemos įstaigai paslaugas ir (ar) produktus pagal sudarytą Sutartį.

4. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

II SKYRIUS
TREČIŲJŲ ŠALIŲ ATITIKTIES VALDYMAS

5. Kibernetinio saugumo reikalavimai nustatomi vadovaujantis šiuo Aprašu ir galiojančiais teisės aktais, reglamentuojančiais kibernetinį saugumą:

5.1. Kibernetinio saugumo įstatymu;

5.2. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" (toliau – Nutarimas Nr. 818);

5.3.Kitais teisės aktais, reglamentuojančiais kibernetinį saugumą ar visuotinai pripažintais gerosios patirties standartais.

6. Trečioji šalis privalo atitikti šiame Apraše ir kituose teisės aktuose nustatytus reikalavimus, kurie perkeliami į sutartis ir viešojo pirkimo dokumentus.

III SKYRIUS
KOKYBĖS REIKALAVIMAI TREČIŲJŲ ŠALIŲ TEIKIAMOMS PASLAUGOMS IR (AR) PRODUKTAMS

7. Valstybinės archyvų sistemos įstaigų darbuotojai, atsakingi už trečiųjų šalių paslaugų ir (ar) produktų įsigijimo inicijavimą, rengdami technines specifikacijas, užduoties aprašymus ar kitus dokumentus turi nustatyti detalius įsigyjamų paslaugų ir (ar) produktų reikalavimus, kokybės vertinimo kriterijus bei SLA:

7.1. Bendrieji kokybės vertinimo kriterijai. Rengiant pirkimo dokumentus ir vertinant trečiųjų šalių teikiamų paslaugų ir (ar) produktų atitiktį, turi būti taikomi šie bendrieji kriterijai (atsižvelgiant į pirkimo pobūdį):

7.1.1. atitiktis techninei specifikacijai – paslaugos ir (ar) produktai turi atitikti pirkimo dokumentuose ir sutartyje nustatytus funkcinius, techninius ir saugumo reikalavimus;

7.1.2. klaidų ir trūkumų valdymas – testavimo ir eksploatacijos metu nustatyti trūkumai turi būti šalinami nustatytais terminais. Priimant produktą klaidų neturi būti.

7.1.3. atitiktis kibernetinio saugumo reikalavimams – paslaugos ir (ar) produktai turi atitikti taikomus kibernetinio saugumo reikalavimus, įskaitant pažeidžiamumų valdymą ir saugumo testavimą;

7.1.4. dokumentacijos pakankamumas – turi būti pateikta išsami, aiški ir aktuali naudotojo, administravimo ir (ar) techninė dokumentacija;

7.1.5. paslaugos prieinamumas – turi būti nustatytas minimalus paslaugos ar sistemos veikimo ir pasiekiamumo rodiklis, ne mažesnis kaip 99,5 proc. per kalendorinį mėnesį (į šį laiką neįskaičiuojant iš anksto suderintų planinių techninės priežiūros darbų);

7.1.6. pagalbos tarnybos prieinamumas – turi būti apibrėžtas pagalbos teikimo darbo laikas (minimalus standartas – įprastomis darbo dienomis nuo 8:00 iki 17:00 val.), o

kritinėms sistemoms – numatyta reagavimo tvarka ir ne darbo metu (24/7);

7.1.7. duomenų atsarginių kopijų valdymas – turi būti nustatytas atsarginių kopijų kūrimo periodiškumas (minimalus standartas – ne rečiau kaip 1 kartą per 24 valandas), o kopijų saugojimo ir atkūrimo reikalavimai turi užtikrinti galimybę atkurti duomenis iš kopijos, darytos ne seniau nei prieš 24 valandas;

7.1.8. ataskaitų teikimas – trečioji šalis turi periodiškai, ne rečiau kaip kartą per ketvirtį, teikti ataskaitas apie paslaugos veikimą, incidentus ir SLA rodiklių laikymąsi.

7.2. Sukurti IT produktai ir (ar) jų valdymas. Įsigyjant programinės įrangos kūrimo, vystymo ar priežiūros paslaugas, pirkimo dokumentuose trečiajai šaliai privaloma nustatyti šiuos minimalius reikalavimus:

7.2.1. perduodamas produktas ar jo versija neturi turėti žinomų kritinių (angl. *Critical*) ar aukšto (angl. *High*) lygio pažeidžiamumų (pagal CVSS ar analogišką vertinimą). Kartu su perdavimu turi būti pateikiama automatinio saugumo skenavimo ataskaita;

7.2.2. trečioji šalis įsipareigoja diegti kritinius saugumo atnaujinimus ne vėliau kaip per 5 darbo dienas nuo jų išleidimo, o kitus saugumo atnaujinimus – ne vėliau kaip per 15 darbo dienų arba pagal atskirai suderintą grafiką.

7.3. Incidentų ir sutrikimų šalinimo SLA. Valstybinei archyvų sistemos įstaigai įsigyjant TIS palaikymo, priežiūros paslaugas, trečioji šalis įsipareigoja registruoti ir šalinti bet kokius TIS veikimo sutrikimus (kibernetinius incidentus ir programinės įrangos klaidas) pagal pirkimo dokumentuose nustatytus reagavimo ir sprendimo terminus. Nustatomi terminai neturi būti ilgesni nei žemiau nurodyti, priklausomai nuo sutrikimo kritiškumo lygio:

Kritiškumo lygis	**Apibūdinimas**	**Reagavimo laikas**	**Sprendimo laikas***
Kritinis	TIS visiškai nepasiekiama arba neveikia pagrindinės funkcijos; nėra laikino sprendimo būdo (angl. *workaround*).	≤ 1 val.	≤ 12 val.
Didelis	Neveikia dalis svarbių TIS funkcijų, tačiau darbas įmanomas (yra laikinas sprendimas) arba TIS veikimas žymiai sulėtėjęs.	≤ 4 val.	≤ 3 d. d.
Vidutinis / Mažas	Programinės įrangos klaidos, netrukdančios pagrindinėms funkcijoms (pvz., atvaizdavimo klaidos), arba TIS pavieniai, mažo poveikio sutrikimai.	≤ 1 d. d.	≤ 10 d. d.

**Pirkimo dokumentuose gali būti nustatytos išimtys, jei sprendimo laikas priklauso nuo trečiųjų šalių gamintojų išleidžiamų pataisų, tačiau tokiu atveju trečioji šalis privalo per nurodytą laiką pateikti laikiną problemos sprendimo būdą).*

8. Į sudaromas sutartis su trečiosiomis šalimis, priklausomai nuo pirkimo pobūdžio, turi būti perkelti visi įsigyjamų paslaugų ir (ar) produktų kokybės vertinimo kriterijai ir SLA, o valstybinės archyvų sistemos įstaigų darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, šiame Apraše nustatyta tvarka turi užtikrinti įsigyjamų paslaugų ir (ar) produktų kokybės vertinimo atitiktį kriterijams ir SLA stebėseną bei fiksavimą.

9. Trečiosios šalies fizinė apsauga užtikrinama vadovaujantis fizinės apsaugos

reikalavimais, nustatytais Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" (toliau – Nutarimas Nr. 818). Sutartyse ar kituose susitarimuose su trečiosiomis šalimis privalo būti iš anksto nustatyta, kad paslaugos teikėjas užtikrina atitiktį kibernetinio saugumo reikalavimams, įskaitant fizinę apsaugą, nustatytiems minėtame apraše. Privaloma užtikrinti ne žemesnį fizinės apsaugos lygį, nei nurodyta valstybinės archyvų sistemos įstaigos Fizinės apsaugos tvarkos apraše

10. Trečioji šalis įsipareigoja saugoti valstybinės archyvų sistemos įstaigų konfidencialią informaciją, pasirašydama konfidencialumo ir duomenų neatskleidimo įsipareigojimus.

11. Valstybinės archyvų sistemos įstaigų kibernetinio saugumo vadovas, priklausomai nuo įsigyjamos paslaugos ir (ar) produktų, turi teisę įsitikinti trečiosios šalies darbuotojų kvalifikacija, prašydamas pateikti atitinkamus kvalifikaciją patvirtinančius įrodymus, leidžiančius dirbti su valstybinės archyvų sistemos įstaigų tinklais ir informacinėmis sistemoms.

12. Valstybinės archyvų sistemos įstaigos turi nustatyti trečiajai šaliai keliamus kvalifikacijos ir pajėgumų reikalavimus. Šie reikalavimai turi būti aiškiai apibrėžti techninėje specifikacijoje, reikalavimų sąvade ar kituose pirkimo dokumentuose.

12.1. Nacionalinio saugumo reikalavimai (privalomi). Vykdant pirkimus, susijusius su valstybinės archyvų sistemos įstaigų TIS ar kibernetinio saugumo užtikrinimu, pirkimo dokumentuose privaloma nustatyti reikalavimą, kad trečioji šalis neturi interesų, galinčių kelti grėsmę nacionaliniam saugumui. Pirkimo dokumentuose nurodomas draudimas dalyvauti trečiosioms šalims (tiekėjams), jų subtiekėjams ar ūkio subjektams, kurių pajėgumais remiamasi, kurie patys ar juos kontroliuojantys asmenys yra registruoti (jeigu tai fizinis asmuo – nuolat gyvenantis ar turintis pilietybę) Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 14 dalyje (arba atitinkamame kitame teisės akte) numatytame sąraše nurodytose valstybėse ar teritorijose.

12.2. Trečiajai šaliai nustatomi kvalifikacijos reikalavimai turi atspindėti perkamos paslaugos ir (ar) produkto pobūdį bei keliamą riziką ir gali apimti:

12.2.1. turimus sertifikatus (pvz., ISO/IEC 27001, ISO/IEC 20000-1 ar kitus su teikiama paslauga tiesiogiai susijusius sertifikatus);

12.2.2. įmonės patirtį teikiant analogiškas ar panašaus sudėtingumo paslaugas ir (ar) produktus (pvz., per pastaruosius 3 metus ir ne mažiau kaip 2 sutartis). Įmonė turi pateikti užsakovų pažymas apie tinkamai įvykdytas ir užbaigtas sutartis;

12.2.3. kitus pajėgumus pagrindžiančius dokumentus, įrodančius gebėjimą saugiai teikti perkamą paslaugą.

12.3. Trečiosios šalies ekspertams, kurie tiesiogiai dirbs su valstybinės archyvų sistemos įstaigų TIS, nustatomi reikalavimai turi būti proporcingi atliekamoms funkcijoms ir gali apimti:

12.3.1. specifinių žinių ar įgūdžių patvirtinimą (pvz., technologijų gamintojų, kibernetinio saugumo ar projektų valdymo sertifikatai, diplomai);

12.3.2. atitinkamą darbo patirtį (pvz., analogiškų paslaugų teikimą ar vadovavimą

projektui) įrodančius dokumentus;

12.3.3. kibernetinio saugumo mokymų baigimą (įskaitant įpareigojimą trečiajai šaliai ne rečiau kaip kartą per metus organizuoti kibernetinio saugumo žinių atnaujinimo mokymus darbuotojams, turintiems prieigą prie valstybinės archyvų sistemos TIS).

12.4. Nustatomi kvalifikacijos ir pajėgumų reikalavimai turi būti tiesiogiai susiję su perkama paslauga ir (ar) produktu, neperteklinіai ir nediskriminaciniai. Trečioji šalis privalo pateikti atitiktį pagrindžiančius dokumentus pirkimo dokumentuose nustatyta tvarka.

13. Pirkimo dokumentuose (techninėje specifikacijoje, reikalavimų sąvade ar kt.) turi būti aiškiai apibrėžti taikytini organizaciniai ir techniniai kibernetinio saugumo reikalavimai. Šie reikalavimai nustatomi atsižvelgiant į planuojamų įsigyti paslaugų ir (ar) produktų pobūdį bei keliamą riziką organizacijos TIS:

13.1. organizaciniai kibernetinio saugumo reikalavimai trečiosioms šalims (pareigos, atsakomybės, kontrolės mechanizmai) nustatomi vadovaujantis šio Aprašo VI skyriaus 25 punktu;

13.2. trečiosios šalies prieiga prie valstybinės archyvų sistemos įstaigų TIS suteikiama tik sutartyje nurodytai paslaugai įgyvendinti, tiksliai apibrėžtam laikotarpiui;

13.3. trečiosios šalies galimi, pagrįsti nukrypimai nuo reikalavimų turi būti aiškiai įvardyti ir dokumentuoti;

13.4. tiek, kiek tai susiję su trečiosios šalies teikiamomis paslaugomis ir turima prieiga prie TIS, trečioji šalis privalo užtikrinti:

13.4.1. žurnalinių įrašų rinkimą, saugojimą ir prieinamumą;

13.4.2. prieigos valdymo kontrolę ar audito vykdymo galimybes;

13.4.3. įsipareigojimus dėl programinės įrangos atnaujinimų vykdymo.

14. Trečioji šalis turi iš anksto pranešti apie bet kokį esminį paslaugų teikimo pakeitimą, įskaitant TIS pakeitimus (pvz., perkėlimas, techninės ar programinės įrangos pakeitimas ir perkonfigūravimas), kurie turi įtakos paslaugų teikimo sutarčiai, informacijos apdorojimui arba saugojimui naujoje geografinėje ar teisinėje jurisdikcijoje, sprendimui naudotis naujų subrangovų paslaugomis (įskaitant esamų subrangovų keitimą).

IV SKYRIUS
TREČIŲJŲ ŠALIŲ TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO RIZIKOS VALDYMAS

15. Valstybinės archyvų sistemos įstaigų prašymu trečioji šalis privalo neatlygintinai sudaryti sąlygas kibernetinio saugumo vadovui arba jo įgaliotam darbuotojui atlikti TIS kibernetinio saugumo rizikos vertinimą bei kitus kibernetinio saugumo patikrinimo veiksmus potencialiems pažeidžiamumams nustatyti.

16. Trečioji šalis privalo neatlygintinai pateikti duomenis, reikalingus patikrinti, ar ji atitinka ir (ar) laikosi sutartyje, kibernetinį saugumą bei asmens duomenų apsaugą reglamentuojančiuose teisės aktuose bei visuotinai pripažintuose gerosios praktikos standartuose nustatytų reikalavimų.

V SKYRIUS

PRIEIGŲ VALDYMAS

17. Trečiųjų šalių prieigos valdomos vadovaujantis Prieigų valdymo tvarkos aprašu, papildomai įgyvendinant šiame Apraše nustatytus reikalavimus.

18. Suteikus trečiajai šaliai fizinę prieigą prie valstybinės archyvų sistemos įstaigų TIS įrenginių ar patalpų arba trečiajai šaliai valstybinės archyvų sistemos įstaigų TIS komponentus (pvz., serverius, duomenų laikmenas) saugant savo patalpose, privaloma:

18.1. užtikrinti trečiosios šalies fizinę apsaugą vadovaujantis fizinės apsaugos reikalavimais pagal Kibernetinio saugumo reikalavimų aprašą;

18.2. užtikrinti ne žemesnį fizinės apsaugos lygį, nei nustatyta Fizinės apsaugos tvarkos apraše.

19. Trečioji šalis gali gauti prieigas prie valstybinės archyvų sistemos įstaigų TIS tik pasirašiusi sutartį ir konfidencialumo, duomenų neatskleidimo įsipareigojimus, įskaitant abiejų šalių atsakomybes dėl valstybinės archyvų sistemos įstaigų informacijos saugumo reikalavimų įgyvendinimo užtikrinimo.

20. Prieigos suteikimo faktas turi būti aprašytas sutartyje, nurodant, kaip identifikuojami asmenys, turėsiantys prieigą prie valstybinės archyvų sistemos įstaigų TIS, taip pat prieigos naudotojų teisės, prieigos laikotarpis ir prieigos aktyvumo periodas (pvz., darbo valandos).

21. Suteikus trečiajai šaliai nuotolinę prieigą prie valstybinės archyvų sistemos įstaigų TIS, privaloma:

21.1. kompiuterinę darbo vietą sukonfigūruoti taip, jog prisijungti prie valstybinės archyvų sistemos įstaigų TIS būtų galima tik naudojant VPN (angl. *Virtual Private Network*) arba alternatyvią, didesnį ar tą patį saugumą užtikrinančią technologiją;

21.2. trečioji šalis privalo užtikrinti, kad darbo vieta, iš kurios vykdomas nuotolinis prisijungimas prie valstybinės archyvų sistemos įstaigų TIS, būtų apsaugota atnaujinta operacine sistema, saugumo pataisomis ir aktyviomis apsaugos priemonėmis, užtikrinančiomis saugų prisijungimą;

21.3. užtikrinti nuolatinę prieigos teisių kontrolę;

21.4. vykdyti nuolatinę veiksmų stebėseną ir kontrolę arba rinkti ir ne trumpiau kaip 90 dienų saugoti žurnalinius įrašus apie atliktus veiksmus, užtikrinant jų vientisumą, konfidencialumą ir prieinamumą pagal pareikalavimą;

21.5. nuotolinė prieiga leidžiama tik suderintais darbo tikslais;

21.6. užtikrinti, kad prisijungimas per nuotolinį ryšį ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „būtina žinoti" bei turėtų sutartą galiojimo terminą, nurodytą sutartyje;

21.7. kiekvienam naudotojui turi būti sukurtas individualus prisijungimo identifikatorius;

21.8. prisijungdama nuotoline prieiga prie valstybinės archyvų sistemos įstaigų TIS trečioji šalis privalo patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksnių tapatumo nustatymo priemonės, angl. *Multi-factor authentication*), jei TIS palaiko tokį funkcionalumą;

21.9. prisijungimo slaptažodis trečiajai šaliai privalo būti perduotas atskirai nuo

naudotojo prisijungimo identifikatoriaus, naudojant saugius ryšio kanalus.

22. Bet kokia nuotolinė prieiga prie valstybinės archyvų sistemos įstaigų TIS, neatitinkanti šiame skyriuje aprašytų reikalavimų, yra draudžiama.

23. Pasibaigus sutarties terminui ar suteikus visas paslaugas prieš sutarties pasibaigimo terminą, trečiųjų šalių prieigos prie valstybinės archyvų sistemos įstaigų TIS turi būti nedelsiant sustabdytos ir (ar) panaikintos.

VI SKYRIUS
SUTARČIŲ SUDARYMO REIKALAVIMAI

24. Valstybinės archyvų sistemos įstaigų darbuotojai, vykdantys viešuosius pirkimus, turi užtikrinti, jog perkant šiame Apraše nurodytas paslaugas ir (ar) produktus pirkimo dokumentai, įskaitant sutarties projektą, būtų derinami su kibernetinio saugumo vadovu.

25. Valstybinės archyvų sistemos įstaigų sutartyse su trečiosiomis šalimis (tiekėjais, įskaitant subtiekėjus), kiek tai susiję su teikiamomis paslaugomis ir (ar) produktais, privaloma numatyti šias pagrindines sąlygas:

25.1. trečiosios šalies atitiktį Kibernetinio saugumo reikalavimų aprašo reikalavimams;

25.2. trečiosios šalies pareigą pranešti kibernetinio saugumo vadovui apie visus didelius ir kitus incidentus, susijusius su valstybinės archyvų sistemos įstaigų TIS, kai tik trečioji šalis sužino apie incidentą, ir neatlygintinai pateikti kibernetinio saugumo vadovui kibernetinio incidento tyrimo ataskaitą pagal valstybinės archyvų sistemos įstaigų Kibernetinių incidentų valdymo tvarkos aprašą;

25.3. trečiosios šalies konfidencialumo ir duomenų neatskleidimo įsipareigojimus pagal valstybinės archyvų sistemos įstaigų Turto valdymo tvarkos aprašą;

25.4. trečiajai šaliai taikomą SLA;

25.5. trečiosios šalies pareigą bendradarbiauti su valstybinės archyvų sistemos įstaigų atsakingais asmenimis kibernetinio saugumo užtikrinimo klausimais bei teikti informaciją ir įrodymus apie reikalavimų įgyvendinimą;

25.6. teisę valstybinės archyvų sistemos įstaigų arba jų įgaliotiems paslaugų teikėjams atlikti trečiosios šalies Kibernetinio saugumo reikalavimų aprašo auditą (įskaitant neplaninį) ir trečiosios šalies pareigą neatlygintinai sudaryti sąlygas tokiam auditui atlikti sutarties vykdymo laikotarpiu ar įvykus dideliam incidentui;

25.7. trečiosios šalies ir valstybinės archyvų sistemos įstaigų teises, pareigas bei atsakomybę dėl kibernetinio saugumo reikalavimų nesilaikymo;

25.8. atsižvelgiant į teikiamos paslaugos ir (ar) produkto specifiką bei valstybinės archyvų sistemos įstaigų TIS keliamą riziką, sutartyse papildomai turi būti numatytos šios specialiosios sąlygos (jei jos taikytinos):

25.8.1. trečiosios šalies personalui būtini įgūdžiai, mokymai, sertifikatai, kvalifikacija;

25.8.2. trečiosios šalies prieigos (loginės ir fizinės) prie TIS lygiai, sąlygos ir suteikimo terminai, vadovaujantis šio Aprašo V skyriumi;

25.8.3. trečiosios šalies pareiga užtikrinti spragų, keliančių riziką valstybinės archyvų sistemos įstaigų TIS, valdymą;

25.8.4. reikalavimai trečiosios šalies patalpoms, įrangai, valstybinės archyvų sistemos įstaigų TIS priežiūrai ir informacijos perdavimui tinklais;

25.8.5. trečiosios šalies pareiga ne rečiau kaip kartą per metus (arba įvykus esminiams pokyčiams / dideliam incidentui) atlikti TIS kibernetinio saugumo rizikos vertinimą ir pateikti ataskaitą bei rizikų valdymo planą;

25.8.6. trečiosios šalies pareiga ne rečiau kaip kartą per metus atlikti atitikties teisės aktams, reglamentuojantiems kibernetinio saugumo valdymą, įsivertinimą;

25.8.7. trečiosios šalies pareiga ne rečiau kaip kartą per metus atlikti TIS veiklos tęstinumo valdymo plano išbandymą;

25.8.8. trečiosios šalies pareiga ne rečiau kaip kartą per 6 mėnesius atlikti TIS spragų testavimą;

25.8.9. trečiosios šalies pareiga leisti valstybinės archyvų sistemos įstaigoms atlikti patikrinimus ar vertinimus (sistemų ar procesų), jei tai būtina atitikčiai patvirtinti.

26. Valstybinės archyvų sistemos įstaigos su interneto paslaugos teikėju turi būti sudariusios sutartis, kuriose būtų numatyta:

- reagavimas į kibernetinius incidentus įprastomis darbo valandomis;
- reagavimas į kibernetinius incidentus po darbo valandų;
- nepertraukiamas interneto paslaugos teikimas: 24 valandas per parą, 7 dienas per savaitę;
- paslaugos sutrikimų registravimas: 24 valandas per parą, 7 dienas per savaitę;
- apsaugos nuo TIS trikdymo taikymas (angl. *Denial of Service, DoS*).

VII SKYRIUS
TREČIŲJŲ ŠALIŲ SĄRAŠO VALDYMAS

27. Valstybinės archyvų sistemos įstaigų darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, rengia ir nuolat atnaujina Trečiųjų šalių sąrašą (2 priedas), kuriame pateikia informaciją apie trečiąją šalį, jos teikiamas paslaugas ir (ar) produktus, atsakingus asmenis, sutartį ir joje numatytus pagrindinius SLA bei įvykusius incidentus.

28. Trečiųjų šalių sąrašas turi būti peržiūrimas ir atnaujinamas inicijuojant numatytus IT ir kibernetinio saugumo reikalavimų pakeitimus naujoms sutartims, pasikeitus sutartims arba įvykus reikšmingiems pokyčiams ar reikšmingiems incidentams, susijusiems su trečiosiomis šalimis.

VIII SKYRIUS
TREČIŲJŲ ŠALIŲ INCIDENTŲ IR TEIKIAMŲ PASLAUGŲ IR (AR) PRODUKTŲ KOKYBĖS VALDYMAS

29. Valstybinės archyvų sistemos įstaigų darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, pateiktame Trečiųjų šalių incidentų ir SLA neatitikčių valdymo registre (3 priedas) turi fiksuoti visus pas trečiąsias šalis įvykusius incidentus ir

SLA neatitikimus, susijusius su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais. Kibernetinio saugumo vadovas privalo pateikti valstybinės archyvų sistemos įstaigų darbuotojui, atsakingam už sutarties įgyvendinimą, reikiamą informaciją apie įvykusius trečiųjų šalių incidentus, turėjusius įtakos trečiųjų šalių teikiamoms paslaugoms ir (ar) produktams, kuriuos naudoja valstybinės archyvų sistemos įstaigos.

30. Valstybinės archyvų sistemos įstaigų darbuotojai, atsakingi už sutarties su trečiosiomis šalimis įgyvendinimą, turi vertinti trečiųjų šalių incidentų ir SLA neatitikčių valdymo registre užfiksuotus trečiųjų šalių SLA neatitikimus, susijusius su trečiųjų šalių teikiamomis paslaugomis ir (ar) produktais. Nustačius, kad nustatyti neatitikimai valstybinės archyvų sistemos įstaigoms yra nepriimtini, inicijuojamas sutartyje numatytų sankcijų taikymas ir (ar) sutarties su trečiąja šalimi nutraukimas.

IX SKYRIUS
BAIGIAMOSIOS NUOSTATOS

31. Sutartyse dėl paslaugų ir (ar) produktų pirkimo privaloma numatyti, kad šio Aprašo reikalavimai yra neatsiejama sutarties dalis. Valstybinės archyvų sistemos įstaigos ir trečioji šalis gali susitarti dėl šiame Apraše nustatytų reikalavimų taikymo papildomais susitarimais.

32. Apraše reikalavimai trečiajai šaliai galioja tol, kol galioja sutartis.

33. Jei kuri nors šio Aprašo nuostata pripažįstama negaliojančia dėl prieštaravimo imperatyvioms teisės aktų nuostatoms, ji keičiama vadovaujantis sutartyje nustatyta tvarka.

34. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba atsiradus esminių pokyčių, galinčių turėti įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

_____

Tiekimo grandinės saugumo
valdymo tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

TIEKIMO GRANDINĖS SAUGUMO VALDYMO TVARKOS PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Tiekimo grandinės saugumo
valdymo tvarkos aprašo
2 priedas

(Trečiųjų šalių sąrašo forma)

TREČIŲJŲ ŠALIŲ SĄRAŠAS

Eil. Nr.	Informacija apie sutartį							Prieiga	Incidentai		Privalomas paslaugų teikimo lygiai (angl. SLA)	
	Trečiosios šalies pavadinimas	**Teikiamos paslaugos ir (ar) produkto pobūdis**	**Trečiosios šalies kontaktinis asmuo**	**Už sutarties vykdymą atsakingas darbuotojas**	**Sutarties numeris**	**Sutarties terminas**	**Kokybės reikalavimai**	**Suteiktos prieigos prie tinklų ir informacinių sistemų**	**Ar įvyko incidentas (Taip/ Ne)**	**Incidentų skaičius**	**Paslaugų prieinamumas proc. (sutartyje)**	**Paslaugų prieinamumas proc. (pagal faktą)**
1	*[Nurodykite trečiosios šalies pavadinimą]*	*[Nurodykite trečiosios šalies teikiamą paslaugą ir (ar) produktą]*	*[Nurodykite trečiosios šalies teikiamą paslaugą ir (ar) produktą]*	*[Už sutarties vykdymą atsakingą darbuotoją]*	*[Nurodykite sutarties numerį]*	*[Nurodykite, kad baisis sutarties galiojimas]*	*[Nurodykite kokybės reikalavimus, pvz. ISO 27001 sertifikatas]*	*[Nurodykite suteiktas prieigas prie tinklų ir informacinių sistemų]*	*[Nurodykite, ar įvyko incidentas (-ai) - Taip arba Ne]*	*[Nurodykite įvykusių incidentų skaičių]*	*[Nurodykite paslaugų prieinamumą, pvz., 99% per mėnesį ar metus]*	*[Nurodykite koks buvo paslaugų prieinamumas pagal faktą po incidentų]*
2												

_____

Tiekimo grandinės saugumo
valdymo tvarkos aprašo
3 priedas

(Trečiųjų šalių incidentų ir SLA neatitikčių valdymo registro forma)

TREČIŲJŲ ŠALIŲ INCIDENTŲ IR SLA NEATITIKČIŲ VALDYMO REGISTRAS

Eil. Nr.		Informacija apie incidentus				Incidentų valdymas								Trečiosios šalies pagalbos tarnyba	
	Trečiosios šalies pavadinimas	**Eil. Nr.**	**Incidento data**	**Incidento aprašymas**	**Incidento lygis - didelis, nedidelis**	**Reakcijos į incidentą laikas (sutartyje)**	**Reakcijos į incidentą laikas (pagal faktą)**	**Problemų sprendimo laikas (sutartyje)**	**Problemų sprendimo laikas (pagal faktą)**	**Maksimalus leistinas nepasiekiamumo laikas (sutartyje)**	**Maksimali leistina nepasiekiamumo trukmė (pagal faktą)**	**Duomenų atsarginės kopijos atkūrimo laikas (sutartyje)**	**Duomenų atsarginės kopijos ir atkūrimo laikas (pagal faktą)**	**Pagalbos tarnybos darbo valandos (sutartyje)**	**Pagalbos tarnybos kontaktai**
1	*[Nurodykite organizacijos pavadinimą, kurioje įvyko incidentas, pvz., UAB „XXX"]*	1,1	*[Nurodykite incidento datą]*	*[Trumpai apibūdinkite incidentą, pvz., XXX IS nepasiekiama. 50 darbuotojų negali vykdyti darbo funkcijų]*	*[Nurodykite kos incidentas įvyko - didelis arba nedidelis]*	*[Nurodykite reakcijos į incidentą laiką remdamiesi sutarties sąlygomis, pvz., per 30 minučių]*	*[Nurodykite reakcijos į incidentą laiką pagal faktą, pvz., 50 minučių]*	*[Nurodykite problemos sprendimo laiką remdamiesi sutarties sąlygomis, pvz., per 4 valandas]*	*[Nurodykite problemos sprendimo laiką pagal faktą, pvz., per 6 valandas]*	*[Nurodykite maksimalų leistinas nepasiekiamumo laiką remdamiesi sutarties sąlygomis, pvz., 1 val. per mėnesį]*	*[Nurodykite maksimalus nepasiekiamumo laiką pagal faktą po incidento pvz., 2 val.]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką remdamiesi sutarties sąlygomis, pvz., per 12 val]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką pagal faktą po incidento, pvz., per 16 val]*	*[Nurodykite Pagalbos tarnybos darbo valandas, pvz., 24/7 arba 8/5]*	*[Nurodykite Pagalbos tarnybos kontaktus, pvz., tel. xxxxx; Interneto adresas: www.xxxx.xxx]*
2		1,2	*[Nurodykite incidento datą]*	*[Eilučių skaičius kuriamas pagal įvykusių incidentų skaičių]*											
3		1.3.	*[Nurodykite incidento datą]*	*[Eilučių skaičius kuriamas pagal įvykusių incidentų skaičių]*											
4	*[Nurodykite organizacijos pavadinimą, kurioje įvyko incidentas, pvz., VšĮ „XXX"]*	2,1	*[Nurodykite incidento datą]*	*[Trumpai apibūdinkite incidentą, pvz., XXX interneto puslapis neveikia]*	*[Nurodykite kos incidentas įvyko - didelis arba nedidelis]*	*[Nurodykite reakcijos į incidentą laiką remdamiesi sutarties sąlygomis, pvz., per 30 minučių]*	*[Nurodykite reakcijos į incidentą laiką pagal faktą, pvz., 50 minučių]*	*[Nurodykite problemos sprendimo laiką remdamiesi sutarties sąlygomis, pvz., per 4 valandas]*	*[Nurodykite problemos sprendimo laiką pagal faktą, pvz., per 6 valandas]*	*[Nurodykite maksimalų leistinas nepasiekiamumo laiką remdamiesi sutarties sąlygomis, pvz., 1 val. per mėnesį]*	*[Nurodykite maksimalus nepasiekiamumo laiką pagal faktą po incidento pvz., 2 val.]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką remdamiesi sutarties sąlygomis, pvz., per 12 val]*	*[Nurodykite duomenų atsarginės kopijos atkūrimo laiką pagal faktą po incidento, pvz., per 12 val]*	*[Nurodykite Pagalbos tarnybos darbo valandas, pvz., 24/7 arba 8/5]*	*[Nurodykite Pagalbos tarnybos kontaktus, pvz., tel. xxxxx; Interneto adresas: www.xxxx.xxx]*

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

TINKLŲ IR INFORMACINIŲ SISTEMŲ ĮSIGIJIMO, PLĖTOJIMO IR PRIEŽIŪROS SAUGUMO, ĮSKAITANT SPRAGŲ VALDYMĄ IR ATSKLEIDIMĄ, TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) įsigijimo, plėtojimo ir priežiūros viso TIS gyvavimo ciklo metu, TIS pokyčių ir pataisų valdymo, TIS saugumo spragų valdymo ir atskleidimo, taikomų techninių reikalavimų užtikrinimo planavimo, organizavimo, vykdymo ir įgyvendinimo kontrolės proceso eigą, atsakingų darbuotojų funkcijas ir atsakomybes, siekiant, kad valstybinės archyvų sistemos įstaigos tinkamai valdytų TIS įsigijimą, plėtojimą ir priežiūrą bei TIS pokyčius ir pataisas, atskleistų ir šalintų esamas ir (ar) žinomas TIS saugumo spragas bei tinkamai įgyvendintų joms keliamus techninius reikalavimus.

2. Šiame Apraše vartojamos sąvokos:

2.1. **Informacinių technologijų pagalbos tarnyba** (angl. *Service desk*) (toliau – IT pagalbos tarnyba) – valstybinės archyvų sistemos įstaigų naudojama informacinė sistema ar programinė įranga informacinių technologijų kreipiniams ir problemoms, kibernetinio saugumo įvykiams ir incidentams bei pokyčiams registruoti ir valdyti; Nesant IT pagalbos tarnybos, gali būti teikiami elektroniniu paštu atsakingam TIS administratoriui;

2.2. **Kibernetinio saugumo vadovas** – asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

2.3. **Pokyčio iniciatorius** – valstybinės archyvų sistemos įstaigos darbuotojas, inicijavęs tinklų ir informacinių sistemų pokytį;

2.4. **Pokyčio vykdytojas** – valstybinės archyvų sistemos įstaigos darbuotojas ar paslaugų teikėjo įgaliotas asmuo, įgyvendinantis tinklų ir informacinių sistemų pokytį;

2.5. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

2.6. **Tinklų ir informacinių sistemų programinės įrangos atnaujinimas** (angl. *release*) – TIS programinės įrangos gamintojo paskelbta informacija apie tinklų ir informacinių sistemų programinės įrangos atnaujinimą ar atnaujinimų rinkinį;

2.7. **Tinklų ir informacinių sistemų programinės įrangos pataisa** (toliau – pataisa) (angl. *patch*) – TIS programinės įrangos atnaujinimas ar atnaujinimų rinkinys, skirtas tinklų ir informacinių sistemų programinei įrangai patobulinti, jos veikimo sutrikimams ir (ar) programiniame kode esančioms klaidoms ir (ar) saugumo spragoms ištaisyti;

2.8. **Tinklų ir informacinių sistemų kūrimas** – TIS diegimo, konfigūravimo, programavimo darbų ir licencijų (jei taikoma) įsigijimas;

2.9. **Tinklų ir informacinių sistemų likvidavimas** – procesas, inicijuojamas panaikinus veiklos funkciją (funkcijas), kuriai vykdyti buvo sukurta TIS;

2.10. **Tinklų ir informacinių sistemų pokytis** – TIS techninės ar programinės įrangos ar programinio kodo pakeitimas, siekiant patobulinti tinklų ir informacinių sistemų funkcionalumą ar pašalinti saugumo spragą;

2.11. **Tinklų ir informacinių sistemų priežiūra** – pokyčiai TIS, nereikalaujantys (arba reikalaujantys minimalių) programavimo / konfigūravimo darbų;

2.12. **Tinklų ir informacinių sistemų saugumas** – TIS pajėgumas tam tikru patikimumo lygiu išlikti atspariems bet kokiam įvykiui, galinčiam sukelti pavojų saugomų, perduodamų ar tvarkomų duomenų arba per tas tinklų ir informacines sistemas teikiamų arba gaunamų paslaugų prieinamumui, autentiškumui, vientisumui ar konfidencialumui;

2.13. **Tinklų ir informacinių sistemų saugumo vertinimas** (toliau – saugumo vertinimas) – tinklų ir informacinių sistemų saugumo vertinimas ar automatizuotas skenavimas, naudojant automatizuotus skenavimo įrankius (toliau – VMS įrankis) (angl. *Vulnerability management scanner*), programinio kodo saugumo vertinimas (angl. *a Code security review*) ar kitų saugumo spragų nustatymo būdų (pvz., įsilaužimų testavimą) įgyvendinimas, siekiant įvertinti, ar TIS neturi esamų ar žinomų saugumo spragų;

2.14. **Tinklų ir informacinių sistemų skenavimas** – TIS saugumo spragų nustatymo ir vertinimo būdas, kai naudojant VMS ir kitus įrankius atliekama TIS, įskaitant, tačiau neapsiribojant, valdomų ir tvarkomų TIS programinę įrangą, programinį kodą, kompiuterizuotas darbo ir gamybos vietas ir kitą įrangą, skenavimas, siekiant nustatyti, ar nėra esamų ar žinomų saugumo spragų;

2.15. **Tinklų ir informacinės sistemos spraga** – TIS trūkumas, įskaitant informacinių ir ryšių technologijų produktų arba informacinių ir ryšių technologijų paslaugų trūkumus, dėl kurio gali įvykti kibernetinis incidentas ar kuriuo gali būti pasinaudota kibernetinei grėsmei kelti;

2.16. **Tinklų ir informacinės sistemos spragų atskleidimas** (toliau – spragų atskleidimas) – procesas, kurio metu įstaiga iš išorinių šaltinių (saugumo tyrėjų, kitų organizacijų ar NKSC) gauna informaciją apie savo valdomose TIS esančias saugumo spragas arba pati jas nustato ir imasi veiksmų nustatytoms spragoms pašalinti;

2.17. **Tinklų ir informacinės sistemos spragų šalinimas** (toliau – spragų šalinimas) veiksmai, atliekami siekiant tinkamai pašalinti nustatytas esamas ar žinomas TIS

spragas (programinės įrangos atnaujinimai, konfigūracijų keitimai, pasiekiamumo ribojamai, atitinkamų techninių priemonių įsigijimas ir diegimas bei kiti veiksmai);

2.18. **Tinklų ir informacinės sistemos spragų valdymas** (toliau – spragų valdymas) – spragų atskleidimas, vertinimas ir šalinimas;

2.19. **Tinklų ir informacinės sistemos spragų vertinimas** (toliau – spragų vertinimas) – veiksmai, atliekami siekiant įvertinti nustatytų esamų ar žinomų spragų keliamą riziką esamoje aplinkoje, pašalinti netikras ar neteisingai identifikuotas spragas (angl. *false positive*), pagal TIS spragų vertinimo klasifikatorių priskiriant TIS prie atitinkamų rizikos lygių;

2.20. **Tinklų ir informacinių sistemų spragų vertinimo klasifikatorius** (angl. *the Common Vulnerability Scoring System Base Score)* (toliau – CVSS) – organizacijos FIRST (angl. *Forum of Incident Response and Security Teams*) parengtas ir tarptautiniu mastu pripažintas techninis standartas, skirtas tinklų ir informacinių sistemų saugumo spragoms įvertinti (aktuali versija https://www.first.org/cvss/v4-0/).

3. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžiamos Kibernetinio saugumo įstatyme.

4. Aprašas taikomas visoms valstybinės archyvų sistemos įstaigų valdomoms TIS, numatytoms Turto valdymo tvarkos apraše.

II SKYRIUS
ATSAKINGŲ PADALINIŲ IR DARBUOTOJŲ FUNKCIJOS IR ATSAKOMYBĖS

5. Kibernetinio saugumo vadovas atsako už:

5.1. šio Aprašo koordinavimą, periodinę peržiūrą ir įgyvendinimo kontrolę;

5.2. kibernetinio saugumo reikalavimų nustatymą ir įgyvendinimo kontrolę TIS įsigijimo, kūrimo, priežiūros ir plėtros (pokyčių bei pataisų valdymo) procesuose;

5.3. TIS saugumo vertinimo įgyvendinimo plano (toliau – spragų nustatymo planas) parengimą, tvirtinimą bei visų TIS saugumo spragų skenavimų organizavimą;

5.4. TIS saugumo vertinimo užduočių rengimą bei saugumo vertinimo ataskaitų iš paslaugų teikėjų gavimą ir vertinimą;

5.5. saugumo spragų, apie kurias informacija gauta iš trečiųjų šalių ar Nacionalinio kibernetinio saugumo centro, tyrimo organizavimą;

5.6. atskleistų saugumo spragų vertinimą (pagal CVSS klasifikatorių) ir registravimą šiame Apraše numatytomis priemonėmis;

5.7. kritinės ir aukštos rizikos lygio TIS saugumo spragų šalinimo inicijavimą ir kontrolę;

5.8. vidutinės ir žemos rizikos lygio TIS saugumo spragų šalinimo plano parengimą ir jo vykdymo pavedimą atsakingiems valstybinės archyvų sistemos įstaigos darbuotojams (TIS administratoriams);

5.9. techninių saugumo reikalavimų, taikomų valstybinės archyvų sistemos įstaigose, įgyvendinimo kontrolę;

5.10. pagalbą ir konsultacijas valstybinės archyvų sistemos įstaigos darbuotojams TIS saugumo vertinimų ir spragų valdymo klausimais.

6. TIS administratorius atsako už:

6.1. TIS kūrimo, įsigijimo, priežiūros, eksploatavimo, plėtros ir likvidavimo techninį organizavimą bei įgyvendinimą;

6.2. kibernetinio saugumo reikalavimų, keliamų TIS, praktinį įgyvendinimą visose TIS gyvavimo ciklo stadijose;

6.3. TIS pokyčių ir pataisų valdymo techninį organizavimą ir įgyvendinimą;

6.4. informacijos apie TIS programinės įrangos (toliau – PĮ) gamintojų paskelbtus atnaujinimus stebėseną, surinkimą ir šių TIS PĮ atnaujinimų diegimo organizavimą šiame Apraše nustatyta tvarka;

6.5. TIS saugumo spragų, įskaitant kibernetinio saugumo vadovo ar paslaugų teikėjų nurodytas spragas, techninį šalinimą šio Aprašo nustatyta tvarka ir terminais;

6.6. informacijos, susijusios su planuojamu TIS saugumo vertinimu (skenavimu), ir kitų reikiamų duomenų pateikimą kibernetinio saugumo vadovui ir paslaugų teikėjams;

6.7. kibernetinio saugumo vadovo bei TIS savininko informavimą apie sėkmingai pašalintas saugumo spragas bei įdiegtus TIS pokyčius.

7. TIS savininkas atsako už:

7.1. TIS įsigijimo inicijavimą ir planavimą;

7.2. TIS įsigijimo rezultatų įvertinimą;

7.3. sprendimo dėl TIS likvidavimo priėmimą;

7.4. sprendimo dėl TIS pokyčių įgyvendinimo bei pokyčio įgyvendinimo plano patvirtinimo priėmimą;

7.5. pokyčių rezultatų įvertinimą.

8. Pokyčio iniciatorius atsako už:

8.1. reikiamų duomenų, susijusių su inicijuojamu pokyčiu, teikimą pokyčių valdymo proceso dalyviams, pokyčio rezultatų atitikties planuotiems rezultatams vertinimą;

8.2. galutinių pokyčio rezultatų įvertinimą ir patvirtinimą;

8.3. TIS pokyčių planavimo eigos fiksavimą šiame Apraše numatytomis priemonėms.

9. Pokyčio vykdytojas atsako už:

9.1. pokyčio įgyvendinimą ir įgyvendinimo eigos kontrolę šiame Apraše nustatyta tvarka ir terminais;

9.2. TIS naudotojų ir kitų suinteresuotų asmenų informavimą apie pokyčius, kurių įgyvendinimo metu galimi TIS darbo sutrikimai;

9.3. pokyčio iniciatoriaus, TIS savininko kibernetinio saugumo vadovo informavimą apie pokyčių eigą ir rezultatus;

9.4. TIS funkcinių, greitaveikos, apkrovos, skenavimo ir kitų testavimų įgyvendinimą arba inicijavimą ir įgyvendinimo kontrolę;

9.5. testinės aplinkos sukūrimą pagal šio Aprašo nustatytus reikalavimus;

9.6. pokyčio ištestavimo testinėje aplinkoje įgyvendinimą arba inicijavimą ir įgyvendinimo kontrolę;

9.7. TIS pokyčių įgyvendinimo eigos fiksavimą šiame Apraše numatytomis priemonėms.

10. Valstybinės archyvų sistemos įstaigų darbuotojai yra atsakingi už kibernetinio saugumo vadovo pavedimų, susijusių su šio Aprašo numatytų techninių reikalavimų vykdymu, saugumo spragų valdymu ir atskleidimu, įgyvendinimą.

III SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ ĮSIGIJIMAS, PLĖTOJIMAS IR PRIEŽIŪRA

11. Šio Aprašo nuostatos yra taikomos visų valstybinės archyvų sistemos įstaigų valdomų TIS įsigijimui, plėtojimui, priežiūrai bei likvidavimui viso TIS gyvavimo ciklo metu. Jei valstybinės archyvų sistemos įstaigos valdo valstybės informacinę sistemą, jai papildomai taikomi Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo ir šio įstatymo įgyvendinamųjų teisės aktų reikalavimai.

12. TIS gyvavimo ciklas – TIS būsenos pokyčių nuo jos sukūrimo / įsigijimo iki veikimo pabaigos visuma.

13. TIS gyvavimo ciklo stadijos:

13.1. TIS įsigijimas;

13.2. TIS eksploatavimas;

13.3. TIS plėtojimas;

13.4. TIS likvidavimas.

14. Prieš įsigyjant TIS, valstybinės archyvų sistemos įstaigos atsakingi darbuotojai turi įvertinti veiklos poreikius, teisės aktų reikalavimus, kibernetinio saugumo reikalavimus. Tam turi būti parengti TIS techniniai reikalavimai, kibernetinio saugumo reikalavimai ir įsigijimo sąlygos.

15. Numatomos įsigyti TIS techniniai reikalavimai aprašomi techninėje specifikacijoje (toliau – specifikacija), numatant atliktų reikalavimų analizės rezultatus, TIS funkcionalumus, duomenų srautus ir integracijų poreikį, funkcinius ir nefunkcinius reikalavimus, tarp jų ir kibernetinio saugumo reikalavimai.

16. Rengiamoje specifikacijoje turi būti numatyti kibernetinio saugumo reikalavimai:

16.1. reikalavimai saugiam programavimui (jei TIS kuriama ar modifikuojama);

16.2. reikalavimai saugumo sistemoms, skirtoms TIS apsaugoti nuo kenkimo programinės įrangos (virusų, šnipinėjimo programų, nepageidaujamo elektroninio pašto);

16.3. reikalavimai kompiuterių tinklo filtravimo įrangai (ugniasienėms, turinio kontrolės sistemoms, įgaliotiesiems serveriams);

16.4. reikalavimai duomenų perdavimo tinklo saugumui (duomenų šifravimui);

16.5. kiti kibernetinės saugos reikalavimai, būtini konkrečios TIS saugumui užtikrinti.

17. Perkant TIS ar jos kūrimo ar priežiūros paslaugas, tiekėjams keliami reikalavimai, kokybės vertinimo kriterijai ir sutartinės sąlygos nustatomos vadovaujantis Tiekimo grandinės saugumo valdymo tvarkos aprašu.

18. Įsigijus TIS ar jos kūrimo, plėtros ar priežiūros paslaugas, pradedamas TIS diegimo etapas, kurio metu:

18.1. atliekamas TIS bandymas testinėje aplinkoje bei saugumo vertinimas (skenavimas), siekiant nustatyti esamas saugumo spragas. Prieš pradedant bandomąją eksploataciją, nustatyti neatitikimai turi būti pašalinti;

18.2. atliekamas TIS diegimas į gamybinę aplinką, kurį vykdo tik įgalioti darbuotojai ar trečiosios šalys;

18.3. atliekama bandomoji eksploatacija funkcionalumui įvertinti;

18.4. vykdomi naudotojų mokymai;

18.5. parengiama TIS naudojimo ir administravimo dokumentacija.

19. TIS įsigijimas laikomas baigtu, kai valstybinės archyvų sistemos įstaigos atsakingi darbuotojai patvirtina, kad TIS diegimas sėkmingai baigtas, TIS visiškai atitinka specifikacijoje numatytus kibernetinio saugumo reikalavimus ir tinkama naudoti gamybinėje aplinkoje.

20. TIS eksploatavimo metu gamybinėje aplinkoje atliekama nuolatinė TIS veikimo stebėsena, TIS reguliariai atnaujinama, atliekami jos saugumo vertinimai ir rizikų analizė. TIS pokyčių valdymas vykdomas vadovaujantis šio Aprašo nuostatomis.

21. Valstybinės archyvų sistemos įstaigose leidžiama naudoti tik Lietuvos vyriausiojo archyvaro patvirtintą PĮ, o PĮ sąrašas peržiūrimas ne rečiau kaip kartą per metus.

22. TIS eksploatavimo metu valstybinės archyvų sistemos įstaigos darbuotojai ir (ar) trečiosios šalys, teikiančios TIS priežiūros paslaugas, turi užtikrinti nuolatinę TIS priežiūrą, laiku reaguoti į TIS sutrikimus ar neveikimą bei per nustatytą terminą pašalinti TIS sutrikimus, neveikimą bei PĮ klaidas.

23. TIS plėtojimo darbai atliekami pagal šiame Apraše apibrėžtą TIS pokyčių valdymo procesą.

24. TIS likvidavimas inicijuojamas panaikinus veiklos funkciją (-as) ar atsiradus kitoms priežastims, dėl kurių TIS tampa nebereikalinga. TIS likvidavimo metu turi būti užtikrintas saugus jose esančių duomenų perkėlimas ar naikinimas.

25. TIS likvidavimo etapo metu:

25.1. informuojami duomenų teikėjai ir duomenų gavėjai;

25.2. valstybinės archyvų sistemos įstaigos interneto svetainėje paskelbiama informacija, kuri toliau nebus apdorojama, atnaujinama, teikiama ar skelbiama;

25.3. TIS sukaupti duomenys perduodami kitoms valstybinės archyvų sistemos įstaigos TIS arba sunaikinami;

25.4. techninės priemonės perduodamos naudoti kitoms valstybinės archyvų sistemos įstaigos TIS arba likviduojamos.

26. Jeigu likviduojama TIS yra įregistruota kaip valstybės informacinė sistema, jos likvidavimo procedūros turi būti vykdomas vadovaujantis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo ir šio įstatymo įgyvendinamųjų teisės aktų reikalavimais.

27. Kuriant, konfigūruojant ar plėtojant TIS, privalo būti taikomi saugaus programavimo principai (saugaus kodo rašymo praktika, programavimo defektų, galinčių lemti saugumo spragas, vengimas). Šie principai taikomi tiek valstybinės

archyvų sistemos įstaigos darbuotojų rašomam kodui, tiek trečiųjų šalių kuriamai programinei įrangai (įskaitant atvirojo kodo komponentus).

28. Už saugaus programavimo principų taikymą ir pirminio programinio kodo (angl. source code) apsaugą nuo neleistino modifikavimo atsako TIS kūrėjas:

28.1. jeigu TIS kuria ar modifikuoja pati įstaiga – už šių priemonių įgyvendinimą yra atsakingas įstaigos TIS administratorius;

28.2. jeigu TIS kuria trečioji šalis, reikalavimai kodo saugumui ir kokybei turi būti numatyti sutartyje vadovaujantis Tiekimo grandinės saugumo valdymo tvarkos aprašu.

29. Patvirtinus ir įdiegus TIS programinę įrangą, turi būti užtikrinta nuolatinė jos priežiūra ir atnaujinimų valdymas:

29.1. reguliariai diegiami išleisti saugumo naujiniai ir (ar) pataisos;

29.2. identifikuotos saugumo spragos vertinamos ir šalinamos teisės aktuose ar sutartyse numatytais terminais;

29.3. nustatytos TIS veikimo klaidos turi būti registruojamos IT pagalbos tarnyboje ir šalinamos pagal nustatytus paslaugų lygio (SLA) reikalavimus.

30. TIS gyvavimo ciklo metu užtikrinant TIS įsigijimą, kūrimą, priežiūrą, plėtrą ir likvidavimą, turi būti vadovaujamasi Lietuvos Respublikos teisės aktų reikalavimais, tarptautiniais standartais (pvz., standartų ISO/IEC 27001, ISO/IEC 20000 grupėmis) bei gerosiomis pasaulinėmis praktikomis. Už visų etapų įgyvendinimą atsako paskirti atsakingi darbuotojai ir į etapų įgyvendinimą įtrauktas kibernetinio saugumo vadovas.

IV SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ POKYČIŲ VALDYMAS

31. TIS pokyčių (toliau – pokytis) gyvavimo ciklo etapai:

31.1. pokyčio planavimas, apimantis pokyčio identifikavimą, inicijavimą, įvertinimą ir patvirtinimą;

31.2. pokyčio įgyvendinimas;

31.3. įgyvendinto pokyčio peržiūra;

31.4. pokyčio užbaigimas.

32. Pokyčio planavimas ir įgyvendinimas organizuojami atsižvelgiant į pokyčių kategorijas:

32.1. **Standartinis pokytis** (angl. *Standard change*) – pokytis, kuriam galima taikyti standartines rutinines procedūras, nes jam atlikti būtini veiksmai yra žinomi, nekelia rizikos kokybiškam TIS paslaugų teikimui arba TIS infrastruktūros veikimui ir nereikalauja papildomų lėšų;

32.2. **Skubus pokytis** (angl. *Emergency change*) – pokytis, skirtas aukščiausio prioriteto TIS sutrikimams arba problemoms šalinti, reikalaujantis ypatingos įvertinimo, patvirtinimo ir atlikimo skubos, taip pat TIS avariniai pokyčiai (pvz., veiklos atkūrimas likviduojant kibernetinio saugumo incidento ar kitų ekstremaliųjų situacijų padarinius);

32.3. **Plėtros pokytis** (angl. *Normal change*) – pokytis, kuriuo kuriamos arba modernizuojamos TIS paslaugos ir su tuo susiję pokyčio atlikimo veiksmai nėra visiškai aiškūs, o pokyčio atlikimas yra susijęs su tam tikra rizika TIS paslaugų teikimui arba visos TIS infrastruktūros veikimui.

33. Pokyčiai identifikuojami analizuojant TIS veiklos poreikius, kuriuos formuoja socialiniai, teisiniai, ekonominiai, technologiniai aspektai ir tendencijos, esama TIS būklė (netinkama konfigūracija, esamos ar žinomos spragos, neatitiktis teisės aktų ir standartų reikalavimams, pasikartojančios TIS veikimo klaidos ir pan.), taip pat TIS naudotojų ir administratorių poreikiai.

34. Pokyčius inicijuoja pokyčio iniciatorius. TIS naudotojai gali TIS savininkui ar kibernetinio saugumo vadovui teikti pasiūlymus dėl reikalingų pokyčių.

35. Pokyčių inicijavimo pagrindai:

35.1. TIS ar jos infrastruktūros tobulinimas;

35.2. TIS plėtra ar modernizavimas;

35.3. elektroninių paslaugų fiziniams ir juridiniams asmenims teikimo tobulinimas ar plėtra;

35.4. TIS tobulinimas ar plėtra atsižvelgiant į TIS naudotojų ir TIS administratorių poreikius;

35.5. kibernetinio saugumo rizikos įvertinimo metu nustatytos rizikos;

35.6. atitikties Kibernetinio saugumo įstatymo ir šio įstatymo įgyvendinamųjų teisės aktų reikalavimams ir Tinklų ir informacinių sistemų kibernetinio saugumo politikos ir jos įgyvendinimą reglamentuojančių vidaus teisės aktų reikalavimams vertinimo metu nustatytos neatitiktys;

35.7. TIS konfigūracijos klaidos;

35.8. kibernetinio saugumo incidentai;

35.9. nustatytos esamos ar žinomos TIS spragos.

36. Standartiniai pokyčiai valdomi taikant supaprastintą tvarką – jie gali būti registruojami ir įgyvendinami iškart, be išankstinio suderinimo su TIS savininku ir kibernetinio saugumo vadovu.

37. Plėtros pokyčius pokyčio iniciatorius privalo iš anksto suderinti su TIS savininkais ir kibernetinio saugumo vadovu bei sudaryti įgyvendinimo grafiką.

38. Skubius pokyčius pokyčio iniciatorius privalo suderinti su kibernetinio saugumo vadovu.

39. Pokyčiai, galintys sutrikdyti ar sustabdyti valstybinės archyvų sistemos įstaigos veiklą, papildomai turi būti suderinti su valstybinės archyvų sistemos įstaigos vadovu ar jo įgaliotu asmeniu.

40. Pokyčio iniciatorius, suderinęs pokyčius nustatytąja tvarka, juos perduoda pokyčių vykdytojui.

41. Prieš pradėdamas įgyvendinti plėtros pokytį, pokyčio vykdytojas turi informuoti TIS naudotojus ir kitus suinteresuotus asmenis apie pokyčius, kurių įgyvendinimo metu galimi TIS darbo sutrikimai. Apie pokyčius turi būti informuojama pokyčius įgyvendinančio subjekto interneto svetainėje, TIS taikomosiose programose ar kitomis priemonėmis (raštu, elektroniniu paštu ir pan.) ne vėliau kaip prieš tris darbo dienas iki planuojamo pokyčio įgyvendinimo pradžios. Šio punkto nuostatų gali būti nesilaikoma, jeigu įgyvendinami skubūs ar standartiniai pokyčiai.

42. Pokyčio vykdytojas plėtros ir skubų pokytį įgyvendina pagal su TIS

savininkais ir kibernetinio saugumo vadovu suderintą pokyčio įgyvendinimo grafiką, juos nuolat informuodamas apie pokyčio eigą ir tarpinius bei galutinius rezultatus. Pokyčio vykdytojas pokyčio metu kontroliuoja pokyčio įgyvendinimo eigą: svarsto pokyčių valdymo proceso dalyvių pasiūlymus, koordinuoja pokytyje dalyvaujančių dalyvių veiksmus, teikia pasiūlymus TIS savininkams, kibernetinio saugumo vadovui, pagal poreikį – valstybinės archyvų sistemos įstaigos vadovui.

43. Įgyvendinto pokyčio peržiūros metu gali būti atliekami TIS funkciniai, greitaveikos, apkrovos, skenavimo ir kiti testavimai.

44. Pokyčiai, galintys sutrikdyti ar sustabdyti TIS darbą, daryti neigiamą įtaką informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti testavimui skirtoje aplinkoje. Pokyčiai darbinėje aplinkoje gali būti vykdomi šio Aprašo numatytu būdu tik išimtiniais atvejais, kai dėl techninių, programinių ar kitų priežasčių pokyčių nėra galimybės patikrinti testavimui skirtoje TIS aplinkoje, ir tik gavus kibernetinio saugumo vadovo leidimą.

45. TIS testavimo aplinkoje neturi būti konfidencialių ir asmens duomenų. TIS testavimo aplinka turi būti atskirta nuo TIS darbinės aplinkos.

46. TIS savininkui nustačius, kad plėtros pokyčių testavimui skirtoje aplinkoje rezultatas atitinka laukiamus rezultatus, pokyčiai gali būti atliekami darbinėje TIS aplinkoje. Standartiniai pokyčiai įgyvendinami darbinėje aplinkoje, taikant iš anksto patvirtintas standartines procedūras, netaikant privalomo bandymo testinėje aplinkoje.

47. Įgyvendinus pokytį, pokyčio vykdytojas turi parengti ir (ar) atnaujinti TIS dokumentaciją (tinklo schemas, TIS struktūrą, duomenų mainų schemas ir pan.).

48. Įgyvendinus pokytį, pokyčio iniciatorius ir pokyčio vykdytojas turi patikrinti (peržiūrėti) TIS konfigūraciją ir TIS būsenos rodiklius, palyginti ir pagal kompetenciją įvertinti, ar pokytis atitinka planuojamus rezultatus. Sudėtingiems ir specifinių pokyčių rezultatams įvertinti gali būti pasitelkti ir kiti organizacijos ar trečiosios šalies (paslaugų teikėjo) kompetentingi specialistai.

49. Pokyčių valdymo proceso dalyviai pokyčių planavimo ir įgyvendinimo eigą fiksuoja šio Aprašo 3 priede numatytoje Pokyčių registro formoje ir (arba) IT pagalbos sistemoje.

50. Už TIS saugumo vertinimo inicijavimą atliekant plėtros pokytį yra atsakingas pokyčio iniciatorius, skubaus pokyčio atveju – kibernetinio saugumo vadovas.

V SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO SPRAGŲ VALDYMAS IR ATSKLEIDIMAS

51. Spragų valdymo objektai yra Turto valdymo tvarkos apraše nurodytų TIS elementai:

51.1. fiziniuose ir virtualiuose serveriuose (toliau – serveriai), esančiuose valstybinės archyvų sistemos įstaigos patalpose arba trečiųjų šalių duomenų centre;

51.2. trečiųjų šalių (toliau – paslaugų teikėjai) debesijos infrastruktūroje (*angl. Infrastructure as a Service – IaaS*), (pvz., VSSA infrastruktūroje), kai tokias paslaugas užsako valstybinės archyvų sistemos įstaiga;

51.3. kompiuterizuotų darbo vietų (toliau – KDV) techninėje įrangoje, kurią valdo valstybinės archyvų sistemos įstaiga;

51.4. aplikacijose (angl. *Applications*), kurias valdo ir (ar) prižiūri valstybinės archyvų sistemos įstaiga;

51.5. duomenų bazėse, kurias valdo ir (ar) prižiūri valstybinės archyvų sistemos įstaiga;

51.6. tinklo techninėje įrangoje, kurią valdo ir (ar) prižiūri valstybinės archyvų sistemos įstaiga;

51.7. įrenginiuose esančių valdiklių ir daviklių (daiktų interneto valdiklių ir daviklių (angl. *Internet of Things*, *IoT*), kuriuos valdo valstybinės archyvų sistemos įstaiga.

52. Atlikus esminius valdomų ir tvarkomų TIS techninės ar programinės įrangos, programinio kodo, KDV ir gamybos vietų ir kitos įrangos pakeitimus (pvz. TIS architektūros ar infrastruktūros keitimus, naujų TIS modulių diegimą ar esminį TIS esamų modulių funkcionalumo keitimą, visų kompiuterizuotų darbo ar gamybos vietų operacinės įrangos diegimą ir pan.), perkeliant juos į gamybinę aplinką, būtina nustatyti, įvertinti ir pašalinti TIS esamas ar žinomas saugumo spragas, t. y., atlikti TIS saugumo vertinimą ir, esant poreikiui, atlikti kibernetinio saugumo rizikos vertinimą vadovaujantis Tinklų ir informacinių sistemų rizikos vertinimo tvarkos aprašu.

53. TIS saugumo vertinimai turi būti atlikti kartu su TIS funkcionalumų, apkrovos ir (ar) kitais vertinimais ar iš karto po jų.

54. Valdomas TIS ar jų dalis draudžiama diegti į gamybinę aplinką, kol nėra pašalintos nustatytos kritinės ar didelės rizikos saugumo spragos.

55. TIS, KDV ir gamybos vietų skenavimai ar kitų saugumo spragų nustatymo būdų (pvz. įsilaužimų testavimų) įgyvendinimas turi būti periodinis, o visų TIS spragų skenavimas atliekamas ne rečiau kaip kas 6 mėnesius, vadovaujantis Kibernetinio saugumo įstatymo ir šio įstatymo įgyvendinamųjų teisės aktų reikalavimais.

56. Kibernetinio saugumo vadovas turi parengti Spragų nustatymo planą, kurio pagrindu organizuojami saugumo vertinimai, jei reikia, tam pasitelkiant paslaugų teikėjus.

57. Už saugumo vertinimo įgyvendinimą yra atsakingas valstybinės archyvų sistemos įstaigos darbuotojas, kuriam kibernetinio saugumo vadovas paveda atlikti saugumo vertinimą, arba trečioji šalis, su kuria valstybinės archyvų sistemos įstaiga yra sudariusi paslaugų teikimo sutartį.

58. Valstybinės archyvų sistemos įstaigos valdomų TIS esamos ir žinomos saugumo spragos gali būti nustatomos gavus informaciją iš techninės ar programinės įrangos gamintojų, informacijos ir kibernetinio saugumo forumų ar kitų šaltinių (pvz., Nacionaliniam kibernetinio saugumo centrui prie Krašto apsaugos ministerijos paviešinus atitinkamą informaciją).

59. Draudžiama naudoti nepatikimus VMS įrankius (ir) nepatikimų gamintojų sukurtus ir palaikomus VMS įrankius. TIS saugumo vertinimo metu naudojami VMS įrankiai turi būti suderinti su kibernetinio saugumo vadovu.

60. TIS saugumo vertinimai atliekami šiuo periodiškumu:

60.1. išorinių paslaugų techninių pažeidžiamumų skenavimas – priėmimo naudoti stadijoje ir po įdiegimo periodiškai, ne rečiau kaip kas 3 mėnesius;

60.2. išorinių paslaugų įsilaužimo testavimas – periodiškai, ne rečiau kaip kas 3 metus;

60.3. vidinių paslaugų ir infrastruktūros techninių pažeidžiamumų skenavimas – priėmimo naudoti stadijoje ir po įdiegimo periodiškai, ne rečiau kaip kas 6 mėnesius;

60.4. vidinių paslaugų įsilaužimo testavimas – periodiškai, ne rečiau kaip kas 3 metus;

60.5. kompiuterizuotų darbo vietų (KDV) saugumo vertinimas – ne rečiau kaip kartą per metus;

60.6. programinio kodo saugumo vertinimas – atliekamas pagal poreikį, vykdant esminius TIS pakeitimus.

61. Detalūs kiekvieno saugumo vertinimo reikalavimai ir apimtis nustatomi kibernetinio saugumo vadovo patvirtintame Spragų nustatymo plane.

62. Koordinuotas spragų atskleidimas:

62.1. Valstybinės archyvų sistemos įstaiga turi turėti viešai paskelbtą kontaktinį kanalą (pvz., el. pašto adresą), kuriuo išoriniai asmenys galėtų pranešti apie nustatytas TIS saugumo spragas;

62.2. Gauti pranešimai turi būti perduodami kibernetinio saugumo vadovui ir įvertinti per 5 darbo dienas nuo gavimo momento;

62.3. Asmeniui, pateikusiam pranešimą, turi būti patvirtintas jo gavimas ir informuojama apie spragos tyrimo eigą;

62.4. Pranešimuose gauta informacija naudojama vadovaujantis Kibernetinio saugumo įstatymo 25 straipsnio reikalavimais.

63. Nustatytos TIS spragos vertinamos pagal CVSS klasifikatorių.

64. Valstybinės archyvų sistemos įstaigos atsakingas darbuotojas ar paslaugų teikėjas atlikęs valstybinės archyvų sistemos įstaigos TIS saugumo vertinimą turi parengti TIS saugumo vertinimo ataskaitą (toliau – ataskaita), kurioje detaliai aprašomos nustatytos saugumo spragos, pateikiant jų aptikimą patvirtinančius įrodymus, jų išnaudojimo galimybes ir rizikos lygį pagal CVSS klasifikatorių, kuris pateiktas Aprašo 1 lentelėje „Saugumo spragų vertinimo balai ir šalinimo laikai pagal CVSS klasifikatorių".

65. Ataskaitoje prie kiekvienos saugumo spragos privaloma pateikti nustatytų saugumo spragų pašalinimo išsamias rekomendacijas.

66. Kibernetinio saugumo vadovas su ataskaita supažindina saugumo vertinimą inicijavusį darbuotoją ir TIS, kuriuose nustatytos saugumo spragos, savininkus.

67. Kibernetinio saugumo vadovas TIS saugumo vertinimo metu nustatytas saugumo spragas turi šalinti šiame Apraše numatyta pataisų valdymo tvarka (VI skyrius), duodamas pavedimus atsakingiems darbuotojams (jei reikia, suderinęs su valstybinės archyvų sistemos įstaigos vadovu).

68. Duodamas pavedimus atsakingiems darbuotojams pašalinti nustatytas saugumo spragas, kibernetinio saugumo vadovas turi nurodyti jų įgyvendinimo

datą, vadovaudamasis šiame Apraše nustatytais pataisų valdymo įgyvendinimo terminais ir saugumo spragų šalinimo terminais.

69. Kibernetinio saugumo vadovas, duodamas pavedimus, atitinkamai įvertina TIS saugumo spragos galimą įtaką kitoms valstybinės archyvų sistemos įstaigos valdomoms TIS ir, jei reikia, inicijuoja arba pats atlieka jų informacijos saugumo rizikos vertinimą.

70. Kibernetinio saugumo vadovas TIS saugumo vertinimo metu nustatytas TIS saugumo spragas registruoja šio Aprašo 2 priede numatytoje TIS saugumo spragų registro formoje ir (ar) IT pagalbos tarnyboje, kur informaciją nuolat atnaujina, siekdamas užtikrinti tinkamą saugumo spragų valdymą.

71. Darbuotojai, atsakingi už nustatytų TIS saugumo spragų šalinimą, vadovaujasi šiame Apraše nustatytais pataisų valdymo įgyvendinimo ir saugumo spragų šalinimo terminais. Kibernetinio saugumo vadovo sprendimu žemos rizikos saugumo spragos gali būti nešalinamos.

72. Jei TIS saugumo spragų šalinimo priemonių nėra, darbuotojai, atsakingi už saugumo spragų šalinimą, pasitarę su kibernetinio saugumo vadovu, planuoja ir įgyvendina kitas galimas saugumo spragų šalinimo priemones (pvz., kompensacines priemones), organizuoja naujų priemonių įsigijimą ar diegimą (prieigų teisių valdymo, įsilaužimų prevencijos, duomenų nutekinimo techninių priemonių ir kt.).

73. Darbuotojai, atsakingi už TIS saugumo spragų šalinimą, nustatytas TIS saugumo spragas turi pašalinti per laiką, numatytą šio Aprašo 1 lentelėje.

1 lentelė. TIS saugumo spragų vertinimo balai pagal CVSS klasifikatorių ir jų šalinimo laikai.

Saugumo spragos rizikos lygis	**CVSS balas nuo iki**	**Įtaka**	**Maksimalus saugumo spragos šalinimo laikas nuo jos nustatymo momento (dienos)**
Kritinis *(angl. critical)*	10.0 – 9.0	Neigiamai paveikiama visos organizacijos ir visų jos klientų veikla.	3
Aukštas *(angl. high)*	8.9 – 7.0	Neigiamai paveikiama visos organizacijos ir kelių jos klientų veikla.	15
Vidutinis *(angl. medium)*	6.9 – 4.0	Neigiamai paveikiami visi vidiniai organizacijos procesai ir (ar) visi vidiniai darbuotojai.	30
Žemas *(angl. low)*	3.9 – 0.1	Neigiamai paveikiami keli vidiniai organizacijos procesai ir (ar) keli vidiniai darbuotojai.	365

74. Darbuotojai, atsakingi už TIS saugumo spragų šalinimą, negalėdami TIS saugumo spragų pašalinti per šio Aprašo 1 lentelėje nustatytą terminą, apie tai informuoja kibernetinio saugumo vadovą, su juo ir su TIS savininku suderindami papildomą spragos šalinimo terminą.

75. Darbuotojai, atsakingi už TIS saugumo spragų šalinimą, organizuoja ir įgyvendina šias TIS saugumo spragų šalinimo veiklas:

75.1. ištaiso techninės ar programinės įrangos klaidas ir atlieka reikiamas konfigūracijas (jei reikia, dėl to kreipiasi į paslaugų tiekėjus), koordinuoja paslaugų teikėjų

atliekamus techninės ar programinės įrangos klaidų šalinimo ir nustatytų keitimo veiklas, užtikrina jų įgyvendinimo kontrolę;

75.2. apriboja TIS, kuriame yra esama ar žinoma saugumo spraga, pasiekiamumą;

75.3. atnaujina PĮ vadovaudamiesi Pataisų valdymo apraše (VI skyrius) nustatyta tvarka ir terminais;

75.4. paruošia ir su TIS savininku suderina konfigūracijų keitimo planą bei užtikrina jo įgyvendinimą;

75.5. inicijuoja reikiamų techninių priemonių įsigijimą, koordinuoja jų diegimą ir užtikrina diegimo kontrolę;

75.6. pagal poreikį atlieka kitas saugumo spragų šalinimo veiklas.

76. Tais atvejais, kai dar nėra programinės įrangos atnaujinimo iš gamintojo ar taikomos priemonės visiškai nepašalina saugumo spragos, ar saugumo spragos švelninimo veiksmai turi įtaką kitoms valstybinės archyvų sistemos įstaigos valdomoms TIS, atlikus kibernetinio saugumo rizikos vertinimą, tokia TIS gali būti naudojamas nepašalinus jos saugumo spragos tik kibernetinio saugumo vadovo sprendimu, šį sprendimą suderinus su TIS savininku.

77. Darbuotojai, atsakingi už TIS saugumo spragų šalinimą, pašalinę saugumo spragą, įstaigos IT pagalbos tarnyboje atlieka atitinkamus įrašus, o apie pašalintas kritines ir didelės rizikos saugumo spragas nedelsiant informuoja kibernetinio saugumo vadovą.

78. Kibernetinio saugumo vadovas turi sekti TIS saugumo spragų šalinimo eigos procesą.

79. Darbuotojai, atsakingi už IT turto valdymą, siekdami, kad organizacijos valdomos TIS būtų tinkamai apsaugotos nuo saugumo spragų, turi tinkamai įgyvendinti IT valdymo procesus (pakeitimų, konfigūracijų ir sąrankos valdymą, pataisymų valdymą, saugų programavimą ir kitus IT valdymo procesus). Kibernetinio saugumo vadovas konsultuoja atsakingus darbuotojus šių procesų įgyvendinimo metu.

80. Šiame Apraše numatytas TIS saugumo spragų valdymo ir atskleidimo procesas turi būti suderintas su Kibernetinių incidentų valdymo plano nuostatomis.

VI SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ PATAISŲ VALDYMAS

81. TIS administratorius turi periodiškai turimomis priemonėmis tikrinti informaciją apie TIS PĮ gamintojų paskelbtus TIS PĮ atnaujinimus.

82. TIS administratorius, nustatęs, kad TIS PĮ gamintojas paskelbė TIS PĮ atnaujinimą, kuris šalina kritinę ar aukštos rizikos saugumo spragą, apie tai turi informuoti kibernetinio saugumo vadovą, nedelsiant inicijuoti TIS PĮ atnaujinimą pagal skubų pokyčio valdymo būdą ir užtikrinti, kad ši TIS PĮ būtų atnaujinta šio Aprašo numatytais terminais. Už TIS PĮ atnaujinimą atsakingas TIS administratorius apie atliktą TIS PĮ atnaujinimą, kuriuo buvo pašalinta kritinė ar aukšto rizikos lygio saugumo spraga, turi nedelsiant informuoti kibernetinio saugumo vadovą.

83. Kibernetinio saugumo vadovas turi imtis veiksmų, siekdamas įsitikinti, kad su TIS PĮ atnaujinimu yra tinkamai pašalinta kritinė ar aukšto rizikos lygio saugumo spraga. Nustačius, kad kritinė ar aukšto rizikos lygio saugumo spraga su TIS PĮ atnaujinimu nebuvo tinkamai pašalinta, jis turi inicijuoti kompensacinių priemonių įgyvendinimą, kad kritine ar aukšto rizikos lygio saugumo spraga nebūtų lengva pasinaudoti.

84. Vidutinės ar žemos rizikos spragų šalinimo atvejais už TIS PĮ atnaujinimą atsakingas TIS administratorius nuo informacijos gavimo momento turi įvertinti galimybes organizuoti TIS PĮ atnaujinimą pagal standartinį ar plėtros pokyčio valdymo būdą bei suderinti su TIS savininku TIS PĮ atnaujinimo planą ir grafiką.

85. Už TIS PĮ atnaujinimą atsakingas TIS administratorius, gavęs TIS savininko sprendimą inicijuoti TIS PĮ atnaujinimą standartiniu ar plėtros pokyčio valdymo būdu, turi atnaujinti TIS PĮ plane nustatytais terminais arba kreiptis į paslaugų tiekėją su prašymu atnaujinti TIS PĮ plane nustatytais terminais.

86. Kibernetinio saugumo vadovas papildomai turi įvertinti, ar suplanuoto TIS PĮ atnaujinimo metu turi būti atliktas saugumo vertinimas ir vientisumo tikrinimas. Jei taip, saugumo vertinimas ir vientisumo tikrinimas atliekami šio Aprašo nustatyta tvarka.

87. Kibernetinio saugumo vadovas turi įvertinti, kad TIS PĮ pataisos, kuriomis yra šalinamos nustatytos saugumo spragos, turi būti bandomos testinėje aplinkoje, prieš jas diegiant į gamybinę aplinką.

88. Kibernetinio saugumo vadovas turi užtikrinti, kad būtų diegiamos tik oficialių TIS PĮ gamintojų saugos pataisos.

89. Draudžiama diegti Saugos pataisas, jei jose aptinkama saugumo spraga arba nustatoma, kad jos gali daryti didesnę žalą TIS, nei jų diegimo nauda.

VII SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ TECHNINIAI KIBERNETINIO SAUGUMO REIKALAVIMAI

90. Kibernetinio saugumo vadovas ir TIS administratoriai privalo užtikrinti, kad valstybinės archyvų sistemos įstaigų valdomoms TIS viso jų gyvavimo ciklo metu būtų taikomi šie techniniai kibernetinio saugumo reikalavimai:

90.1. TIS turi turėti aktualią tinklų ir informacinių sistemų infrastruktūros loginę schemą ir visų tinklų ir informacinių sistemų schemas (atnaujinti joms pasikeitus);

90.2. Įsilaužimo atakų pėdsakai (angl. *attack signature*) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu įstaigos sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio veiklai vertinimas (testavimas);

90.3. Turi būti įdiegtos ir veikti įsibrovimo aptikimo sistemos, kurios stebėtų į tinklų ir informacinę sistemą įeinantį ir iš jos išeinantį duomenų srautą;

90.4. Valstybinės archyvų sistemos įstaigų vidinės tinklų ir informacinės sistemos turi būti atskirtos nuo viešųjų ryšių tinklų, naudojant saugasienę;

90.5. Saugasienės saugumo taisyklės turi būti nuolat peržiūrimos ir prireikus atnaujinamos. Detali saugasienės taisyklių analizė turi būti atliekama ne rečiau kaip kartą per 6 mėnesius.

90.6. Serveriuose (įskaitant ir virtualias mašinas) ir darbo stotyse turi būti įjungtos ir sukonfigūruotos saugasienės, kontroliuojančios visą įeinantį ir išeinantį srautą;

90.7. Iš išorės gaunami elektroniniai laiškai turi būti filtruojami, siekiant aptikti ir blokuoti kenksmingą turinį;

90.8. Techninės ir programinės įrangos, skirtos kibernetiniams incidentams aptikti, konfigūracijos taisyklės turi būti saugomos elektronine forma atskirai nuo tinklų ir informacinių sistemų techninės įrangos (kartu nurodant atitinkamas įgyvendinimo ar atnaujinimo datas, atsakingus asmenis, taikymo periodus);

90.9. Prisijungiant prie belaidžio tinklo (jeigu jungiamasi prie tinklų ir informacinės sistemos vidinio tinklo), turi būti taikomas tinklų ir informacinių sistemų naudotojų tapatumo patvirtinimo EAP (angl. *Extensible Authentication Protocol*) / TLS (angl. *Transport Layer Security*) protokolas arba naujesnis protokolas, visuotinai pripažįstamas saugiu;

90.10. Tinklui valdyti turi būti naudojami saugūs tinklo protokolai;

90.11. Turi būti uždrausti / išjungti visi nebūtini protokolai ir atviri prievadai (angl. *port*);

90.12. Kompiuteriuose, mobiliuosiuose įrenginiuose turi būti išjungtas lygiarangis (angl. *peer to peer*) funkcionalumas, jei tai nėra reikalinga darbo funkcijoms atlikti;

90.13. Turi būti diegiami naudojamos programinės įrangos gamintojų ir operacinių sistemų rekomenduojami atnaujinimai;

90.14. Tinklų ir informacinės sistemos, dėl objektyvių priežasčių naudojančios nepalaikomas operacinių sistemų ir kitos programinės įrangos versijas, turi veikti atskirame tinklo segmente, atskirtame nuo pagrindinių įstaigos veiklos funkcijų;

90.15. Vidinis įstaigos kompiuterių tinklas turėtų būti segmentuotas, jame atskiriant bent:

90.15.1. tinklų ir informacinių sistemų valdymo ir administravimo potinklį;

90.15.2. atskirą potinklį kiekvienai trečiajai šaliai arba kitais būdais užtikrinant trečiųjų šalių prieigą tik prie tai šaliai reikalingų resursų, kur įmanoma taikant kelių veiksnių prisijungimo autentifikaciją. Prisijungimas turi būti atliekamas naudojant saugų virtualųjį privatų tinklą (angl. *Virtual private network*, VPN). Prisijungimas registruojamas įvykių registravimo žurnaluose;

90.15.3. tinklinių daugiafunkcių įrenginių bei spausdintuvų ir skenerių potinklį;

90.15.4. IP telefonijos potinklį;

90.15.5. darbo vietų potinklį;

90.15.6. testavimo potinklį.

90.16. Mobiliuosiuose įrenginiuose ir kompiuterinėse darbo vietose turi būti naudojamos vykdomojo kodo (angl. *Executable code*) kontrolės priemonės, kuriomis apribojamas neleistino vykdomojo kodo naudojimas ar informuojamas administratorius apie neleistino vykdomojo kodo naudojimą;

90.17. Turi būti parengti ir įdiegti kompiuterinių darbo vietų (įskaitant nešiojamuosius įrenginius) operacinių sistemų atvaizdai ir (arba) kitos priemonės su integruotomis 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 spragų ar atakų. Pagal parengtus atvaizdus į kompiuterines darbo vietas (įskaitant nešiojamuosius įrenginius) turi būti įdiegiama operacinė sistema su saugumo nuostatomis;

90.18. Svetainės serveriuose draudžiama saugoti sesijos duomenis (identifikatorių) prisijungimo tikslams, pasibaigus susijungimo sesijai;

90.19. Internetu prieinamoms svetainėms, tinklų ir informacinėms sistemoms turi būti naudojama svetainės saugasienė (angl. *Web Application Firewall*);

90.20. Internetu prieinamoms svetainėms, tinklų ir informacinėms sistemoms turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų remiantis OWASP (angl. *The Open Worldwise Application Security Project*) Top 10 geriausiomis praktikomis (www.owasp.org);

90.21. Žiniatinklio (angl. *Web*) formose turi būti naudojama svetainės naudotojo įvedamų duomenų kontrolė (angl. *Input validation*);

90.22. Internetu prieinamos tinklų ir informacinės sistemos neturi rodyti naudotojui klaidų pranešimų apie tinklų ir informacinės sistemos ir programinį kodą ar serverį;

90.23. Internetu naudojant HTTPS protokolą (angl. *HyperText Transfer Protocol Secure*, HTTPS) prieinamos tinklų ir informacinės sistemos saugumo priemonės turi leisti tik jų funkcionalumui užtikrinti reikalingus protokolo metodus;

90.24. Įstaigos serveriuose ir kompiuterinėse darbo vietose turi būti naudojamos (jei įmanoma, centralizuotai) valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, stebėjimo realiu laiku priemonės;

90.25. Naudojama tik legali ir leistina (pagal įstaigos patvirtintą sąrašą) programinė įranga;

90.26. Nuolatos turi būti stebimas tinklų ir informacinių sistemų įrangos laisvos atminties ar vietos diske kiekis, apkrova, resursų naudojimas. Pasiekus nustatytas ribines reikšmes, apie tai turi būti informuojami atsakingi asmenys.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

91. Visi valstybinės archyvų sistemos įstaigos valdomų TIS darbuotojai privalo laikytis šio Aprašo reikalavimų.

92. Valstybinės archyvų sistemos įstaigos darbuotojai turi užtikrinti, kad TIS įsigijimo, kūrimo, priežiūros ir plėtros, TIS saugumo vertinimų, TIS saugumo spragų valdymo ir atskleidimo planavimo ir įgyvendinimo veiksmai atitiktų šio Aprašo nuostatas.

93. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba įvykus esminiai pokyčių, galinčių turėti įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

_____

Tinklų ir informacinių sistemų įsigijimo,
plėtojimo ir priežiūros saugumo,
įskaitant spragų valdymą ir atskleidimą,
tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

TINKLŲ IR INFORMACINIŲ SISTEMŲ ĮSIGIJIMO, PLĖTOJIMO IR PRIEŽIŪROS SAUGUMO, ĮSKAITANT SPRAGŲ VALDYMO IR ATSKLEIDIMO, TVARKOS APRAŠO PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	Statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, tvarkos aprašo
2 priedas

(Tinklų ir informacinių sistemų saugumo spragų registro forma)

TINKLŲ IR INFORMACINIŲ SISTEMŲ SAUGUMO SPRAGŲ REGISTRAS

Nr.	Spragos atskleidimo data	Tikrintas objektas	Spragos aprašymas	Spragos vertinimas	Spragos šalinimo terminas iki	Spragos šalinimo veikla	Kompensacinė priemonė ir kitas veiksmas	Atsakingas padalinys / darbuotojas / trečioji šalis	Spragos šalinimo statusas	Spragos pašalinimo data	Pastabos
1	2	3	4	5	6	7	8	9	10	11	12

[*Pildymo instrukcija.*
[1] nurodomas spragos eilės numeris;
[2] nurodoma spragos atskleidimo data;
[4] aprašoma atskleista spraga (pvz., naudojamas nesaugus duomenų perdavimo sertifikatas „PAVADINIMAS" ir pan.);
[5] nurodomas spragos vertinimas balais ir pavadinimu pagal CVSS klasifikatorių, vadovaujantis Aprašo 1 lentelėje numatytais saugumo spragų rizikos lygiais (pvz. 9.0 balai kritinis rizikos lygis);
[6] nurodomas spragos šalinimo laikas, vadovaujantis Aprašo 1 lentelėje numatytais saugumo spragų šalinimo laikais (pvz. per 24 val.);
[7] pateikiamas spragos šalinimo veiklos aprašymas, kuris gali būti paimtas iš skenavimo ataskaitos rekomenduojamų veiksmų (pvz., nesaugaus duomenų perdavimo sertifikato „PAVADINIMAS" pakeitimas į saugų „PAVADINIMAS");
[8] nurodomas kompensacinės priemonės ar kitos veiklos, kuri bus įgyvendinama laikinai, kol bus pašalinta saugumo spraga, pavadinimas (pvz., IT paslaugos patalpinimas į DMZ zoną);
[9] nurodomas už spragos pašalinimą ar kompensacinės priemonės pritaikymą atsakingo padalino pavadinimas, darbuotojo pareigos, vardas ir pavardė ar paslaugų teikėjo, kuriam pavesta pašalinti spragą, pavadinimas;
[10] nurodomas vienas iš spragos šalinimo statusų: (i) Planuojama; (ii) Vykdoma; (iii) Pašalinta;
[11] nurodoma spragos pašalinimo data;
[12] jei reikia, pateikiamos pastabos ar komentarai.

_____

Tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, tvarkos aprašo
3 priedas

(Tinklų ir informacinių sistemų pokyčių registro forma)

TINKLŲ IR INFORMACINIŲ SISTEMŲ POKYČIŲ REGISTRAS

Nr.	Pokyčio pavadinimas	Pokyčio objektas	Pokyčio iniciatorius	Pokyčio kategorija	Sudėtingumo lygis	Planuojama įgyvendinimo data ir laikas	Sprendimą priimantis asmuo	Sprendimo statusas	Pokyčio vykdytojas	Pokyčio vykdymo statusas	Pokyčio įvykdymo data	Pastabos
1	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**	**10**	**11**	**12**	**13**

[*Pildymo instrukcija.*
[1] nurodomas pokyčio numeris;
[2] nurodomas pokyčio pavadinimas (pvz., TIS programinės įrangos atnaujinimas);
[3] nurodomas TIS pavadinimas, kaip ji vadinama organizacijoje (pvz., finansų valdymo TIS);
[4] nurodomos pokyčio iniciatoriaus pareigos, vardas ir pavardė;
[5] nurodoma viena iš Apraše numatytų pokyčio kategorijų: (i) Standartinis pokytis; (ii) Skubus pokytis; (iii) Plėtros pokytis;
[6] nurodoma vienas iš Apraše numatytų pokyčio sudėtingumų lygių: (i) Aukštas sudėtingumas; (ii) Vidutinis sudėtingumas; (iii) Žemas sudėtingumas;
[7] nurodoma planuojama pokyčio įgyvendinimo data arba laiko terminas (pvz., iki liepos 5 d. arba nuo liepos 5 d. 9 val. iki 17 val.);
[8] nurodomos sprendimą dėl pokyčio įgyvendinimo priimančio darbuotojo pareigos, vardas ir pavardė;
[9] nurodomas sprendimo dėl pokyčio įgyvendinimo priėmimo statusas: (i) laukiama; (ii) patvirtinta; (iii) atmesta;
[10] nurodomos pokyčio vykdytojo pareigos, vardas ir pavardė arba paslaugos teikėjo pavadinimas;

[11] nurodomas pokyčio vykdymo statutas: (i) Planuojamas; (ii) Vykdomas; (iii) Atidėtas; (iv) Įvykdytas;
[12] nurodoma pokyčio įvykdymo data ir laikas, jei būtinas;
[13] jei reikia, pateikiamos pastabos ar komentarai.

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

KIBERNETINIO SAUGUMO REIKALAVIMŲ VEIKSMINGUMO VERTINIMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) kibernetinio saugumo reikalavimų, nustatytų Lietuvos Respublikos kibernetinio saugumo įstatyme ir Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo" (toliau – Kibernetinio saugumo reikalavimų aprašas), įgyvendinimo stebėseną, matavimą, analizę ir įvertinimą.

2. Aprašas taikomas visoms valstybinės archyvų sistemos įstaigų valdomoms tinklų ir informacinėms sistemoms, kibernetinio saugumo valdymo procesams bei taikomoms kibernetinio saugumo organizacinėms ir techninėms priemonėms, skirtoms mažinti kibernetinio saugumo riziką ir užtikrinti kibernetinio saugumo reikalavimų įgyvendinimą.

3. Apraše naudojamos sąvokos:

3.1. **Atitikties vertinimas** – kibernetinio saugumo reikalavimų atitikties Kibernetinio saugumo įstatymo ir Kibernetinio saugumo reikalavimų aprašo bei Lietuvos vyriausiojo archyvaro tarnybos patvirtintiems kibernetinio saugumo politikos dokumentuose nustatytiems reikalavimams vertinimas, atliekamas vadovaujantis Kibernetinio saugumo reikalavimų aprašo VIII skyriaus reikalavimais;

3.2. **Kibernetinio saugumo vadovas** – asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

3.3. **Kontrolės priemonės** – techniniai, organizaciniai ir procedūriniai veiksmai, skirti mažinti informacijos saugumo riziką ir užtikrinti kibernetinio saugumo reikalavimų įgyvendinimą ir užtikrinimą;

3.4. **Rodiklis** – matavimo vienetas, naudojamas kibernetinio saugumo reikalavimų įgyvendinimo veiksmingumui ir tikslų pasiekimui vertinti;

3.5. **Stebėsenos planas** – šio Aprašo pagrindu parengtas, su valstybės archyvų vadovais suderintas ir Lietuvos vyriausiojo archyvaro patvirtintas Kibernetinio saugumo reikalavimų įgyvendinimo ir užtikrinimo stebėsenos planas;

3.6. **Kompensacinės priemonės –** laikinos organizacinės ar techninės

kibernetinio saugumo priemonės, taikomos tol, kol pašalinama nustatyta neatitiktis Kibernetinio saugumo įstatymo, Kibernetinio saugumo reikalavimų aprašo ar valstybinės archyvų sistemos įstaigų kibernetinio saugumo politikos dokumentų reikalavimams. Kompensacinės priemonės turi sumažinti neatitikties keliamą kibernetinio saugumo riziką iki priimtino lygio ir negali būti laikomos nuolatiniais neatitikties šalinimo sprendimais. Kompensacines priemones nustato Kibernetinio saugumo vadovas ir jos įtraukiamos į Neatitikčių šalinimo planą kartu su planuojama neatitikties pašalinimo data.

3.7. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.

4. Valstybinės archyvų sistemos įstaigos turi užtikrinti reikiamus išteklius kibernetinio saugumo reikalavimų įgyvendinimo veiksmingumo stebėsenos ir vertinimo veikloms vykdyti.

II SKYRIUS
ATITIKTIES VERTINIMAS

5. Kibernetinio saugumo vadovas su valstybinės archyvų sistemos įstaigos darbuotoju, atsakingu už kibernetinio saugumo reikalavimų įgyvendinimą, ne rečiau kaip kartą per metus vykdo atitikties vertinimą. Tam gali būti pasitelkiamos trečiosios šalys.

6. Kibernetinio saugumo vadovas turi parengti Atitikties vertinimo ataskaitą (vertinimas gali būti atliekamas Kibernetinio saugumo informacinės sistemos (toliau – KSIS) savideklaracijos klausimyno pagrindu) ir identifikuotų neatitikčių šalinimo planą, kuriame turi būti siūlomi už neatitikčių šalinimo veiksmus atsakingi darbuotojai ir (ar) padaliniai, reikalingi ištekliai ir šalinimo veiksmų įgyvendinimo terminai (toliau – Neatitikčių šalinimo planas). Kibernetinio saugumo vadovo parengtą Atitikties vertinimo ataskaitą ir Neatitikčių šalinimo planą, suderinęs su valstybės archyvų vadovais, tvirtina Lietuvos vyriausiasis archyvaras. Iki bus įgyvendinti Neatitikčių šalinimo plane numatyti veiksmai, valstybinės archyvų sistemos įstaigos pagal galimybes turi taikyti kompensacines priemones.

7. Kibernetinio saugumo vadovas po atitikties vertinimo turi ne rečiau kaip kartą per metus pateikti atitikties vertinimo rezultatus, KSIS užpildydamas Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos (toliau – NKSC) klausimyną.

8. Atitikties vertinimo rezultatų bei Neatitikčių šalinimo plano pagrindu, atsižvelgus į kibernetinio saugumo rizikų vertinimo rezultatus, nustatomos prioritetinės stebėsenos sritys ir sudaromas šio Aprašo III skyriuje numatytas Stebėsenos planas.

9. Kibernetinio saugumo vadovas, vadovaudamasis Kibernetinio saugumo įstatymo 14 straipsnio 8 punkto nuostatomis, ne rečiau kaip kartą per 3 metus turi organizuoti valstybinės archyvų sistemos įstaigų kibernetinio saugumo audito atlikimą. Kibernetinio saugumo auditas turi būti atliktas pagal NKSC patvirtintą kibernetinio saugumo auditų

atlikimo metodiką. Kibernetinio saugumo auditą turi atlikti nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti informacinių sistemų saugumo atitikties auditoriai, audito įmonės ar kitos institucijos, NKSC vadovo nustatyta tvarka mokymus išklausę ir kvalifikacinius žinių ir praktinių įgūdžių patikrinimo egzaminą išlaikę asmenys, atitinkantys NKSC kibernetinio saugumo auditų atlikimo metodikoje nustatytus nepriklausomumo, nešališkumo ir nepriekaištingos reputacijos reikalavimus (toliau kartu – Auditoriai). Auditoriams negali būti pavedama vertinti TIS, kurias valdo ir (ar) tvarko subjektas, kuriame dirba Auditorius, kibernetinio saugumo valdymo.

10. Atlikus kibernetinio saugumo auditą, Auditorius turi parengti ir kibernetinio saugumo vadovui pateikti kibernetinio saugumo audito ataskaitą, su kuria kibernetinio saugumo vadovas turi supažindinti valstybinės archyvų sistemos įstaigų vadovus ir kitas suinteresuotas šalis. Kibernetinio saugumo vadovas per 10 darbo dienų nuo kibernetinio saugumo audito ataskaitos pateikimo dienos turi parengti ir, suderinęs su valstybės archyvų vadovais, Lietuvos vyriausiajam archyvarui teikti tvirtinti kibernetinio saugumo audito metu nustatytų neatitikčių (jei nustatyta) šalinimo planą, kuriame turi būti nurodyti už šalinimo veiksmus atsakingi darbuotojai ir (ar) padaliniai, reikalingi ištekliai ir šalinimo veiksmų įgyvendinimo terminai.

11. Kibernetinio saugumo auditų ataskaitas bei identifikuotų neatitikčių (jei nustatyta) šalinimo planai turi būti saugomi ne mažiau kaip 3 metus nuo jų patvirtinimo.

12. NKSC, atlikdamas valstybinės archyvų sistemos įstaigos patikrinimą, turi teisę jos pareikalauti pateikti atliktų kibernetinio saugumo audito, atitikties vertinimo ataskaitos, atitikties vertinimo metu nustatytų neatitikčių šalinimo plano, rizikų vertinimo ataskaitos ir rizikų valdymo plano kopijas. Kibernetinio saugumo vadovas šiuos dokumentus turi pateikti į KSIS ne vėliau kaip per 5 darbo dienas nuo NKSC prašymo gavimo dienos.

III SKYRIUS
KIBERNETINIŲ SAUGUMO REIKALAVIMŲ ĮGYVENDINIMO STEBĖSENA, MATAVIMAS, ANALIZĖ IR VERTINIMAS

13. Remiantis Atitikties ir Rizikų vertinimo rezultatais, kibernetinio saugumo reikalavimų stebėsenai, matavimui, analizei ir įvertinimui užtikrinti yra rengiamas valstybinės archyvų sistemos įstaigos Stebėsenos planas (2 priedas). Kibernetinio saugumo vadovas Stebėsenos planą turi teikti tvirtinti Lietuvos vyriausiajam archyvarui, prieš tai suderinęs su valstybės archyvų vadovais.

14. Kibernetinio saugumo vadovas Stebėsenos planą rengia atsižvelgdamas į:

14.1. kibernetinio saugumo rizikos vertinimo rezultatus;

14.2. kibernetinio saugumo reikalavimų atitikties Kibernetinio saugumo įstatymo ir atitikties vertinimo rezultatus;

14.3. kibernetinio saugumo audito, atliekamo vadovaujantis Kibernetinio saugumo įstatymo 14 straipsnio 8 dalies nuostatomis, rezultatus;

14.4. kibernetinio saugumo reikalavimų pasiekimo būklę;

14.5. valstybinės archyvų sistemos įstaigos kibernetinių incidentų pobūdį ir skaičių;

14.6. trečiųjų šalių paslaugų teikėjams iškeltus kibernetinio saugumo reikalavimus;

14.7. valstybinės archyvų sistemos įstaigos veiklos procesų pokyčius.

15. Stebėsenos plane turi būti nurodyta:

15.1. nustatoma kibernetinio saugumo reikalavimų stebima sritis;

15.2. kibernetinio saugumo reikalavimų nustatytos srities rodikliai (metrikos), kurie bus stebimi, siekiant vertinti kibernetinio saugumo kontrolės priemonių veiksmingumą ir jų įtaką nustatytoms rizikoms mažinti. Tokie rodikliai gali apimti, pavyzdžiui:

15.2.1. kibernetinių incidentų skaičių ir jų sprendimo laiką;

15.2.2. kibernetinių incidentų aptikimo laiką;

15.2.3. saugumo atnaujinimų (angl. *patches*) įdiegimo laiką ir procentinę dalį;

15.2.4. kelių veiksnių autentifikavimo (MFA) naudojimo procentą;

15.2.5. darbuotojų kibernetinės higienos testų ar fišingo simuliacijų rezultatus;

15.2.6. pažeidžiamumų skenavimo metu nustatytų spragų skaičių ir jų pašalinimo laiką;

15.2.7. atsarginių kopijų kūrimo ir atkūrimo testavimo rezultatus;

15.2.8. saugumo auditų ir atitikties vertinimų metu nustatytų neatitikčių skaičių ir jų pašalinimo laiką.

15.3. pasirinkto kibernetinio saugumo reikalavimų rodiklio siekiama reikšmė;

15.4. už pasirinkto kibernetinio saugumo reikalavimų rodiklio stebėseną atsakingas organizacijos darbuotojas arba padalinys;

15.5. už kibernetinio saugumo reikalavimų veiklos įgyvendinimą atsakingas organizacijos darbuotojas arba padalinys;

15.6. stebimo kibernetinio saugumo reikalavimų rodiklio įverčio rezultatas – pasiektas ar nepasiektas;

15.7. stebimo kibernetinio saugumo reikalavimų rodiklio įverčio rezultato aplinkybės.

16. Kibernetinio saugumo vadovas Stebėsenos planą peržiūri ir, jei reikia, atnaujina ne rečiau kaip kartą per metus.

17. Kibernetinio saugumo reikalavimų veiksmingumui vertinti gali būti taikomi šie stebėsenos, matavimo ir analizės metodai:

17.1. saugumo įvykių ir žurnalinių įrašų (angl. *logs*) analizė;

17.2. saugumo įvykių valdymo sistemų (angl. *SIEM*) generuojamų įspėjimų (angl. *alerts*) analizė;

17.3. pažeidžiamumų skenavimo ir saugumo testavimo rezultatų analizė;

17.4. kibernetinių incidentų registravimo ir valdymo statistikos analizė;

17.5. saugumo kontrolės priemonių veikimo ir efektyvumo testavimas;

17.6. atsarginių duomenų kopijų atkūrimo testavimo rezultatų analizė;

17.7. kibernetinio saugumo auditų ir atitikties vertinimų rezultatų analizė;

17.8. darbuotojų kibernetinės higienos mokymų ir testavimo rezultatų analizė.

18. Valstybinės archyvų sistemos įstaigos darbuotojas, atsakingas už Stebėsenos plane numatytų rodiklių stebėjimą, informaciją apie rodiklių būklę suveda į Stebėsenos planą jame numatytais terminais.

19. Kibernetinio saugumo vadovas ne rečiau kaip kartą per metus arba įvykus reikšmingiems incidentams ar pokyčiams rengia Stebėsenos plano rodiklių pasiekimų ataskaitą, kurioje apibendrinamos nustatytų rodiklių pokyčių tendencijos ir jų įtaka valstybinės archyvų sistemos įstaigos kibernetinio saugumo rizikos lygiui.

20. Kibernetinio saugumo vadovas, įvertinęs, kad stebimas kibernetinio saugumo reikalavimų rodiklis neatitinka nustatytų reikšmių, turi nustatyti neatitikties priežastį ir atitinkamai pakoreguoti neatitikčių šalinimo planą.

21. Lietuvos vyriausiasis archyvaras ar jo įgalioti darbuotojai, peržiūrėję Stebėsenos plano rodiklių pasiekimų ataskaitą, įvertina valstybinės archyvų sistemos įstaigų kibernetinio saugumo būklę, priima sprendimus dėl papildomų kibernetinio saugumo priemonių įgyvendinimo ir, jei reikia, paveda imtis veiksmų nustatytoms rizikoms mažinti.

22. Stebėsenos plano duomenys vertinami pagal kibernetinio saugumo reikalavimų pasiekimo lygį – ar nustatytas lygis pasiektas, ar ne.

23. Remiantis Stebėsenos plano rezultatais turi būti peržiūrimas Valstybinės archyvų sistemos įstaigų rizikos valdymo priemonių planas ir, esant poreikiui, koreguojami konkrečių priemonių įgyvendinimo prioritetai arba numatomos naujos kontrolės priemonės.

IV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

24. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba atsiradus esminių pokyčių, galinčių turėti įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas Kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

25. Visi su kibernetinio saugumo reikalavimų stebėsena susiję įrodymai turi būti saugomi užtikrinant jų konfidencialumą, vientisumą ir prieinamumą tik valstybinės archyvų sistemos įstaigos įgaliotiems darbuotojams, kurie dalyvauja kibernetinio saugumo reikalavimų stebėsenos, matavimo, analizės ir įvertinimo procese.

26. Valstybinės archyvų sistemos įstaigų darbuotojai, dalyvaujantys kibernetinio saugumo reikalavimų stebėsenos, matavimo, analizės ir įvertinimo procese, privalo laikytis šio Aprašo reikalavimų.

_____

Kibernetinio saugumo reikalavimų
veiksmingumo vertinimo tvarkos
1 priedas

(Apskaitos žurnalo forma)

KIBERNETINIO SAUGUMO REIKALAVIMŲ VEIKSMINGUMO VERTINIMO TVARKOS PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Kibernetinio saugumo reikalavimų
veiksmingumo vertinimo tvarkos
2 priedas

(Kibernetinio saugumo reikalavimų įgyvendinimo ir užtikrinimo stebėsenos plano forma)

KIBERNETINIO SAUGUMO REIKALAVIMŲ ĮGYVENDINIMO IR UŽTIKRINIMO STEBĖSENOS PLANAS

Eil. Nr.	Stebima sritis	Rodiklis	Vertinama	Rezultatas	Siekiama reikšmė	Stebėjimo dažnumas	Atsakingas už stebėjimą darbuotojas/ padalinys	Atsakingas už veiklos įgyvendinimą darbuotojas/ padalinys	Įverčiai (pasiekta/ nepasiekta)			
									[metai]	Komentaras (aplinkybės)	[metai]	Komentaras (aplinkybės)

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

KIBERNETINĖS HIGIENOS PRAKTIKOS ORGANIZAVIMO IR KIBERNETINIO SAUGUMO MOKYMŲ ORGANIZAVIMO IR VYKDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) kibernetinės higienos reikalavimus bei kibernetinio saugumo mokymų organizavimą.

2. Apraše vartojamos sąvokos:

2.1. **Kibernetinio saugumo vadovas** – asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

3. **Konfidenciali informacija –** valstybinės archyvų sistemos įstaigų disponuojama ir saugoma nevieša, vertinga informacija, fiksuojama popierine ar elektronine forma, bei viešai neskelbtini asmens duomenys, kurių atskleidimas gali sukelti neigiamą poveikį organizacijai ar tretiesiems asmenims, įskaitant fizinius asmenis.

4. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Kibernetinio saugumo įstatyme.

5. Kibernetinio saugumo vadovas turi užtikrinti, kad ne rečiau kaip kartą per metus visi valstybinės archyvų sistemos įstaigų darbuotojai išklausytų kibernetinės higienos praktikos mokymus.

II SKYRIUS
SU ŽMOGIŠKŲJŲ IŠTEKLIŲ VALDYMU SUSIJĘS KIBERNETINIS SAUGUMAS

6. Visi naujai priimami į darbą ir esami valstybinės archyvų sistemos įstaigų darbuotojai privalo susipažinti su Tinklų ir informacinių sistemų (toliau – TIS) kibernetinio saugumo politika bei jos įgyvendinamaisiais dokumentais ir įsipareigoti jų laikytis.

7. Pasibaigus valstybinės archyvų sistemos įstaigų valstybės tarnautojo ar darbuotojo, dirbančio pagal darbo sutartį (toliau – darbuotojas), valstybės tarnybos ar darbo santykiams, darbuotojas privalo grąžinti jam išduotą TIS techninę įrangą Turto valdymo tvarkos aprašo nustatyta tvarka.

8. Prieiga prie TIS suteikiama, stabdoma ar naikinama bei periodiškai peržiūrima pagal darbuotojo pareigas ir atsakomybę Prieigų valdymo tvarkos aprašo nustatyta tvarka.

9. Fizinė įėjimo ir išėjimo iš darbo vietos kontrolė vykdoma Fizinės apsaugos tvarkos aprašo nustatyta tvarka.

10. Kibernetinio saugumo incidentai valdomi vadovaujantis Kibernetinių incidentų valdymo planu. Darbuotojas, pastebėjęs galimą kibernetinį incidentą ar saugumo pažeidimą, privalo nedelsiant apie tai informuoti Kibernetinio saugumo vadovą ir TIS administratorių.

III SKYRIUS
ŠVARAUS STALO IR ŠVARAUS EKRANO SAUGUMAS

11. Laikinai palikdamas kompiuterinę darbo vietą darbuotojas privalo „užrakinti" savo kompiuterį, įjungdamas ekrano užsklandą su slaptažodžiu.

12. TIS administratorius užtikrina, kad kompiuteriai automatiškai *„užsirakintų"* ne vėliau kaip po 15 min. neaktyvumo, išskyrus tuos atvejus, kai yra būtinybė užtikrinti nepertraukiamą darbo vietos veikimą (pvz., apsaugos postuose, klientų savitarnos terminaluose).

13. Darbuotojas privalo užtikrinti, kad jo darbo vietoje laikoma konfidenciali informacija būtų apsaugota nuo neteisėto atskleidimo. Jeigu darbo vietoje yra spinta ar stalčius, kuriame laikoma konfidenciali informacija, jie turi būti uždaryti, o darbuotojui pasišalinus – užrakinti. Tvarkant įslaptintą informaciją privaloma vadovautis Lietuvos Respublikos valstybės ir tarnybos paslapčių įstatymo ir šio įstatymo įgyvendinamųjų teisės aktų reikalavimais.

14. Darbuotojui draudžiama laikyti slaptažodžius spausdinta ar kita rašytine formoje viešai ant darbo stalo ar šalia kompiuterio.

15. Dokumentai, kuriuose yra konfidencialios informacijos, privalo būti paimti iš spausdintuvo dėklo iš karto po atspausdinimo.

IV SKYRIUS
KIBERNETINIO SAUGUMO MOKYMŲ ORGANIZAVIMAS

16. Kibernetinio saugumo vadovas kiekvienų metų IV ketvirtį organizuoja visų valstybinės archyvų sistemos įstaigų darbuotojų kibernetinio saugumo mokymus.

17. Darbuotojų kibernetinio saugumo mokymai planuojami pagal Lietuvos vyriausiojo archyvaro patvirtintą darbuotojų mokymų planą, suderintą su valstybinės archyvų sistemos įstaigų vadovais.

18. Mokymų plane turi būti numatyti šie gyvai ar nuotoliniu būdu vykdomi mokymai:

18.1. bendrieji kibernetinės saugos higienos praktikos mokymai visiems darbuotojams šiomis temomis: teisinė atsakomybė ir duomenų apsauga; fizinis saugumas; „švaraus stalo" politika; saugus darbas iš namų; socialinė inžinerija; saugūs slaptažodžiai ir jų valdymas; mobiliųjų įrenginių saugumas; geroji kibernetinio saugumo praktika; kibernetinių incidentų registravimas;

18.2. specializuoti kibernetinio saugumo mokymai TIS administratoriams šiomis temomis: tinklų saugumas; spragų valdymas ir atskleidimas; saugus TIS konfigūravimas; žurnalinių įrašų valdymas; kriptografijos raktų valdymas; atsarginių duomenų kopijų

valdymas; kibernetinių incidentų valdymas; prieigų valdymas; kibernetinio saugumo priemonių administravimas;

18.3. specializuoti kibernetinio saugumo mokymai vadovams šiomis temomis: kibernetinio saugumo pagrindai (sąvokos, principai, grėsmės, saugos valdymas ir pan.); teisinė atsakomybė; kibernetinio saugumo kultūros kūrimas; kibernetinio saugumo ir informacijos saugumo integracija į verslo veiklos procesus; finansinių ir žmogiškųjų išteklių paskirstymas; kibernetinio saugumo rizikų valdymas; saugumo politika ir technologinės apsaugos valdymas; kibernetinių incidentų valdymas; kiti svarbūs žingsniai kibernetinio saugumo link.

19. Kibernetinio saugumo vadovas per 3 mėnesius po kibernetinio saugumo klausimais organizuotų mokymų turi parengti ir patvirtinti mokymų ataskaitą, kurioje turi būti nurodyta mokymų tema ir dalyvių skaičius. Mokymų ataskaita saugoma ne mažiau kaip 3 metus nuo jos užregistravimo datos.

20. Suderinusi su Kibernetinio saugumo vadovu, kibernetinio saugumo mokymus nurodytomis temomis gali organizuoti pati valstybinės archyvų sistemos įstaiga, arba gali juos įsigyti iš trečiųjų šalių – paslaugų teikėjų.

21. Kibernetinio saugumo vadovas informuoja valstybinės archyvų sistemos įstaigos darbuotojus apie kibernetinio saugumo aktualijas:

21.1. el. paštu siųsdamas saugumo pranešimus ar rekomendacijas;

21.2. skelbdamas aktualijas vidiniame portale ar kitaip apribotame žiniatinklyje;

21.3. per vidines bendravimo platformas, tokias kaip „*Microsoft Teams*“ ir pan.;

21.4. pristatydamas informaciją susirinkimų metu;

21.5. įvairia informacine medžiaga darbo vietoje (plakatai, lipdukai, kortelės).

22. Valstybinės archyvų sistemos įstaigų vadovai ar jų įgalioti asmenys privalo papildomai ne rečiau kaip kartą per 2 metus Nacionalinio kibernetinio saugumo centro vadovo nustatyta tvarka išklausyti kibernetinio saugumo mokymus ir užtikrinti valstybinės archyvų sistemos įstaigų darbuotojų nuolatinį švietimą kibernetinio saugumo srityje.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

23. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba atsiradus esminių pokyčių, galinčių turėti įtakos šiam Aprašui. Už Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas Kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal priede nustatytą apskaitos žurnalo formą.

_____

Kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

KIBERNETINĖS HIGIENOS PRAKTIKOS ORGANIZAVIMO IR KIBERNETINIO SAUGUMO MOKYMŲ ORGANIZAVIMO IR VYKDYMO TVARKOS APRAŠO PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

KRIPTOGRAFIJOS IR ŠIFRAVIMO NAUDOJIMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Kriptografijos ir šifravimo naudojimo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) kriptografinių priemonių, šifravimo metodų ir kriptografinių raktų valdymo principus, siekiant užtikrinti perduodamos ir saugomos informacijos konfidencialumą, vientisumą ir autentiškumą.

2. Apraše vartojamos sąvokos:

2.1. **Kibernetinio saugumo vadovas** – asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

2.2. **Šifravimas** – kriptografinis elektroninės informacijos formos pakeitimas iš paprastos į specifinę, iš kurios elektroninę informaciją pakeisti į pradinę formą galima tik turint atitinkamą kriptografijos raktą.

3. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Kibernetinio saugumo įstatyme.

4. Už šio Aprašo reikalavimų įgyvendinimą ir priežiūrą atsakingas Kibernetinio saugumo vadovas, o už techninį šifravimo priemonių ir kriptografinių raktų diegimą bei administravimą – TIS administratorius.

II SKYRIUS
KRIPTOGRAFIJOS IR ŠIFRAVIMO PRIEMONIŲ NAUDOJIMAS

5. Valstybinės archyvų sistemos įstaigose naudojamos tik visuotinai saugiomis pripažintos kriptografinės technologijos, algoritmai, raktų ilgiai ir protokolų versijos, kurių sąrašas pateiktas Aprašo 2 priede.

6. Kriptografijos priemonės parenkamos atsižvelgiant į valstybinės archyvų sistemos įstaigų informacijos klasifikaciją ir kibernetinio saugumo rizikos vertinimo rezultatus.

7. Viešaisiais elektroninių ryšių tinklais perduodamos valstybinės archyvų sistemos įstaigų jautrios informacijos konfidencialumas turi būti užtikrinamas naudojant duomenų šifravimą (pvz.: TLS) arba virtualų privatų tinklą (VPN).

8. Belaidis ryšys valstybinės archyvų sistemos įstaigose turi būti apsaugotas naudojant:

8.1. saugius šifravimo algoritmus (draudžiama naudoti TKIP ar WEP, privaloma naudoti AES pagrindu veikiančius algoritmus);

8.2. rekomenduojamo ilgio šifravimo raktus (ne trumpesnius kaip 128 bitų);

8.3. naujausias saugias belaidžio ryšio protokolų versijas (pavyzdžiui, WPA2-Enterprise, WPA3 arba, kai to neleidžia techninės galimybės ar tinklo paskirtis, – WPA2-Personal su ne trumpesniu kaip 12 simbolių sudėtingu slaptažodžiu).

9. Belaidės prieigos stotelėse privaloma pakeisti standartinius gamintojo nustatytus slaptažodžius ir šifravimo raktus.

10. Duomenys darbo stotyse, mobiliuosiuose įrenginiuose ir išorinėse laikmenose turi būti šifruojami pagal šio Aprašo III skyriuje nustatytus reikalavimus.

11. Draudžiama naudoti pasenusias arba nesaugias šifravimo technologijas, kurios laikomos pažeidžiamomis pagal kibernetinio saugumo gerąją praktiką. Draudžiamų algoritmų ir protokolų sąrašas pateiktas Aprašo 2 priede.

12. Slaptažodžiai duomenų bazėse, sistemose ar aplikacijose negali būti saugomi atviru tekstu – juos privaloma paversti maišos reikšmėmis (angl. *hashed*), naudojant saugius, skaičiavimo resursams imlius maišos algoritmus, pateiktus Aprašo 1 priede.

13. Valstybinės archyvų sistemos įstaigose naudojamos kriptografinės technologijos, algoritmai, raktų ilgiai ir protokolai turi būti periodiškai peržiūrimi, atsižvelgiant į technologijų raidą, naujai nustatytas saugumo spragas ir tarptautinių standartizacijos organizacijų rekomendacijas.

14. Nustačius, kad naudojamas kriptografinis algoritmas, protokolas ar raktų ilgis neatitinka saugumo reikalavimų ar yra laikomas nesaugiu, valstybinės archyvų sistemos įstaigos privalo planuoti ir įgyvendinti jo pakeitimą saugesne technologija per protingą ir rizika pagrįstą laikotarpį.

15. Tais atvejais, kai valstybinės archyvų sistemos įstaigos duomenys tvarkomi trečiųjų šalių informacinėse sistemose, debesų kompiuterijos paslaugose ar perduodami paslaugų teikėjams, turi būti užtikrinama, kad naudojamos kriptografinės apsaugos priemonės atitiktų šio Aprašo reikalavimus arba būtų lygiavertės saugumo požiūriu.

III SKYRIUS
DUOMENŲ ŠIFRAVIMAS DARBO STOTYSE, MOBILIUOSIUOSE ĮRENGINIUOSE IR LAIKMENOSE

16. Duomenys, perduodami tarp mobiliojo įrenginio ir valstybinės archyvų sistemos įstaigų tinklų ar informacinių sistemų, turi būti šifruojami naudojant virtualų privatų tinklą (VPN) su TLS sertifikatu arba privataus prieigos taško (APN) technologiją per mobiliojo ryšio operatorių, taikant TLS šifravimą, kai VPN technologija nėra palaikoma.

17. Visų valstybinės archyvų sistemos įstaigų mobilių įrenginių ar kitų iš įstaigos patalpų išnešamų darbo stočių kietieji diskai privalo būti pilnai šifruoti (angl. *Full Disk Encryption*), pvz., naudojant „BitLocker" ar analogišką technologiją.

18. Išorinėse kompiuterinėse laikmenose (USB laikmenose, išoriniuose diskuose ir kt.) saugomi valstybinės archyvų sistemos įstaigos duomenys turi būti šifruojami.

IV SKYRIUS
INTERNETO SVETAINIŲ KRIPTOGRAFIJOS REIKALAVIMAI

19. Valstybinės archyvų sistemos įstaigų interneto svetainėse ir kitose WEB

pagrindu veikiančiose aplikacijose turi būti įgyvendinti šie kriptografijos reikalavimai:

19.1. naudojami oficialiai pripažinti saugūs raktų ilgiai;

19.2. atliekant svetainės administravimo darbus ryšys turi būti šifruojamas;

19.3. šifravimui naudojami skaitmeniniai sertifikatai turi būti išduoti patikimų sertifikavimo tarnybų;

19.4. naudojamas TLS standartas (1.2 versija arba naujesnė);

19.5. svetainės kriptografinės funkcijos turi būti įdiegtos serverio dalyje, kuriame talpinama svetainė, arba kriptografiniame saugumo modulyje (angl. *Hardware Security Module – HSM*);

19.6. visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. *fail securely*).

V SKYRIUS
ATSARGINIŲ KOPIJŲ ŠIFRAVIMAS

20. Duomenys atsarginėse kopijose turi būti šifruojami.

21. Atsarginių kopijų šifravimo raktai turi būti saugomi atskirai nuo atsarginių kopijų laikmenų.

22. Jei dėl techninių apribojimų nėra galimybės užšifruoti atsarginių kopijų (pvz., pasenusios informacinės sistemos (*angl. legacy software*)), turi būti taikomos kitos techninės ar organizacinės priemonės, kurios neleistų neteisėtai atkurti kopijose saugomos informacijos.

VI SKYRIUS
KRIPTOGRAFINIŲ RAKTŲ VALDYMAS

23. Valstybinės archyvų sistemos įstaigose turi būti užtikrinamas saugus kriptografinių raktų valdymas.

24. Kriptografinių raktų valdymas apima:

24.1. raktų generavimą (raktai privalo būti generuojami naudojant patikimus, kriptografiškai saugius pseudoatsitiktinių skaičių generatorius; naudojamų kriptografinių raktų ilgiai ir algoritmai turi atitikti Aprašo 2 priede nustatytus reikalavimus);

24.2. raktų paskirstymą (raktai ir sertifikatai gali būti perduodami asmenims ar techninėms sistemoms tik saugiais kanalais, užtikrinant jų vientisumą ir konfidencialumą (pvz., naudojant šifruotą ryšį, o asimetrinės kriptografijos atveju – atskiriant viešojo ir privataus rakto perdavimą); privačius raktus draudžiama siųsti atviru tekstu el. paštu ar per viešas susirašinėjimo platformas);

24.3. raktų saugojimą (raktai (duomenų bazių šifravimo ar atsarginių kopijų raktai) privalo būti logiškai arba fiziškai atskirti nuo duomenų, kuriuos jie šifruoja; šifravimo raktus draudžiama saugoti atviru tekstu tame pačiame kataloge ar duomenų bazėje kartu su užšifruotais duomenimis, tinklo šifravimo (TLS) privatūs raktai turi būti saugomi specialiai tam skirtose apribotos prieigos operacinės sistemos direktorijose, raktų saugyklose (angl. *Key Vault)* arba aparatiniuose saugumo moduliuose (angl. *HSM)*);

24.4. raktų naudojimą (raktai turi būti naudojami tik tam tikslui, kuriam jie buvo sukurti (pavyzdžiui, skaitmeninio parašo raktas negali būti naudojamas duomenų

šifravimui) ir TIS administratorius privalo užtikrinti, kad prieiga prie raktų naudojimo būtų suteikiama vadovaujantis principais „būtina žinoti" (angl. *Need to know*) ir „mažiausių privilegijų" (angl. *Least privilege*);

24.5. raktų archyvavimą (TIS administratorius privalo užtikrinti kritinių raktų, įskaitant atsarginių kopijų iššifravimo raktus, atsarginių kopijų darymą ir saugų jų saugojimą fiziškai ar logiškai izoliuotoje aplinkoje, užtikrinant galimybę atkurti duomenis praradus pagrindinį raktą);

24.6. raktų sunaikinimą (pasibaigus rakto galiojimo laikui, paaiškėjus, kad raktas arba asmens kompiuteris galėjo būti kompromituotas, arba kai duomenys, kuriems jis buvo skirtas, nebesaugomi, raktas turi būti nedelsiant atšauktas ir saugiai sunaikintas iš visų laikmenų, užtikrinant, kad jo nebūtų galima atkurti);

25. Praradus kriptografinį raktą arba įtariant jo sukompromitavimą, apie tai nedelsiant turi būti informuojamas Kibernetinio saugumo vadovas.

26. Kibernetinio saugumo vadovas privalo nedelsiant imtis priemonių galimai rizikai sumažinti, įskaitant rakto panaikinimą, pakeitimą ar prieigos apribojimą.

27. Kriptografinio rakto sukompromitavimas arba įtariamas kriptografinės apsaugos pažeidimas laikomas informacijos saugumo incidentu ir turi būti valdomas Kibernetinių incidentų valdymo tvarkos apraše nustatyta tvarka.

VII SKYRIUS
AUDITAS IR STEBĖSENA

28. Valstybinės archyvų sistemos įstaigose turi būti saugomi ir stebimi audito įrašai, susiję su kriptografinių raktų valdymo veikla.

29. Audito įrašuose turi būti registruojama:

29.1. kriptografinių raktų generavimas;

29.2. raktų naudojimas;

29.3. raktų archyvavimas;

29.4. raktų sunaikinimas;

29.5. naudotojų veiksmai, susiję su raktų valdymu.

30. Audito įrašai turi būti saugomi laikantis Žurnalinių įrašų valdymo tvarkos aprašu.

VIII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

31. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba atsiradus esminių pokyčiai, galinčių turėti įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas Kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

_____

Kriptografijos ir šifravimo
naudojimo tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

KRIPTOGRAFIJOS IR ŠIFRAVIMO NAUDOJIMO TVARKOS PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	**Veiklos data**	**statusas**	**Atsakingas asmuo**	**Pagrindinės korekcijos**	**Patvirtinimo data ir Nr.**

_____

Kriptografijos ir šifravimo
naudojimo tvarkos aprašo
2 priedas

PATVIRTINTŲ IR DRAUDŽIAMŲ KRIPTOGRAFINIŲ ALGORITMŲ SĄRAŠAS

Patvirtinti kriptografiniai algoritmai

1. Simetrinis šifravimas:
   1.1. AES-256 – PRIVALOMAS kritiniams duomenims
   1.2. AES-128 – LEIDŽIAMAS vidutinės svarbos duomenims
   1.3. ChaCha20-Poly1305 – LEIDŽIAMAS mobiliesiems įrenginiams ir našumo kritiškoms sistemoms
2. Asimetrinis šifravimas ir parašai:
   2.1. RSA ≥ 3072 bitų (rekomenduojama 4096)
   2.2. ECDSA ≥ 256 bitų
   2.3. Ed25519 – LEIDŽIAMAS
3. Raktų apsikeitimo algoritmai:
   3.1. ECDH ≥ 256 bitų
   3.2. X25519 – LEIDŽIAMAS
4. Maišos funkcijos:
   4.1. SHA-256 – MINIMALUS reikalavimas
   4.2. SHA-384, SHA-512 – REKOMENDUOJAMOS kritinėms sistemoms
   4.3. SHA-3 – LEIDŽIAMA
   4.4. BLAKE2 – LEIDŽIAMA
5. Slaptažodžių maišos algoritmai:
   5.1. bcrypt su cost faktoriumi ≥ 12;
   5.2. scrypt;
   5.3. Argon2id – REKOMENDUOJAMA.

Draudžiami algoritmai ir protokolai

6. Šie algoritmai yra GRIEŽTAI DRAUDŽIAMI dėl žinomų saugumo spragų:
   6.1. MD5;
   6.2. SHA-1;
   6.3. DES, 3DES;
   6.4. RC4;
   6.5. RSA su raktu < 2048 bitų;
   6.6. Bet kokie savarankiškai sukurti šifravimo algoritmai.
7. Draudžiami protokolai:
   7.1. Visi SSL protokolai (SSLv2, SSLv3);
   7.2. TLS 1.0;
   7.3. TLS 1.1.

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

FIZINĖS APSAUGOS TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Fizinės apsaugos tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) už fizinę apsaugą atsakingo darbuotojo funkcijas ir atsakomybes, patalpų kategorijoms keliamus reikalavimus ir darbuotojų įsipareigojimus, taikomus valstybinės archyvų sistemos įstaigų fizinei apsaugai užtikrinti.

2. Aprašo tikslas – nustatyti fizinės apsaugos reikalavimus valstybinės archyvų sistemos įstaigų patalpoms.

3. Aprašu siekiama užtikrinti:

3.1. tinkamą prieigų suteikimą įėjimui į patalpas, kuriose įrengta tinklų ir informacinių sistemų (toliau – TIS) įranga, serveriai ar naudotojų ir administratorių darbo vietos (toliau – patalpos);

3.2. tinkamą patalpų saugumą.

4. Apraše vartojamos sąvokos:

5. **Už fizinę saugą atsakingas asmuo** – valstybinės archyvų sistemos įstaigos darbuotojas, atsakingas už fizinę apsaugą valstybinės archyvų sistemos įstaigoje.

5.1. **„Švaraus stalo" politika** – Lietuvos vyriausiojo archyvaro nustatyta tvarka, įpareigojanti darbuotojus darbo vietose nepalikti nesaugomos informacijos (dokumentų, laikmenų, įrenginių ar kitų duomenų laikmenų) pasitraukus iš darbo vietos. Ši politika skirta sumažinti neteisėtos prieigos rizikai ir užtikrinti, kad informacija nebūtų palikta atvirai prieinama.

5.2. **Budėtojas** – saugos tarnybos ar valstybinės archyvų sistemos įstaigos darbuotojas, atsakingas už įėjimo į organizacijos teritoriją, pastatą ar patalpas kontrolę, atvykstančių ir išeinančių asmenų (ir (ar) transporto) fiksavimą.

5.3. **Fizinė apsauga** – administracinių, organizacinių, fizinių, technologinių saugumo priemonių visuma, užtikrinanti apsaugą nuo neteisėto patekimo į valstybinės archyvų sistemos įstaigų teritoriją ir patalpas bei saugomos informacijos apsaugą nuo konfidencialumo, vientisumo ar prieinamumo pažeidimo. Fizinė apsauga taikoma atsižvelgiant į saugomos informacijos svarbą valstybinės archyvų sistemos įstaigose, šios informacijos apimtį ir teritoriją, patalpų ar darbo vietų priskyrimą atitinkamai saugos zonai.

5.4. **Fizinio saugumo priemonės** – fizinės (rakinama spinta, durys, grotos ant langų ir kt.) ir technologinės (biometrinė prieigos kontrolė, vaizdo stebėjimo kameros, dokumentų smulkintuvas, apsaugos signalizacija, automatinis durų rakinimas, automatinė gaisro aptikimo sistema ir kt.) priemonės, skirtos užkirsti kelią neteisėtam asmenų patekimui į saugomas patalpas ar teritorijas, neteisėtam susipažinimui su šiose vietose saugoma informacija ir kitiems neteisėtiems šių asmenų veiksmams bei informacijai apsaugoti nuo konfidencialumo, vientisumo ir prieinamumo pažeidimo.

5.5. **Kibernetinio saugumo vadovas** – asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas.

6. Kitos šiame Apraše vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Kibernetinio saugumo įstatyme.

7. Aprašo reikalavimų privalo laikytis visi valstybinės archyvų sistemos įstaigų darbuotojai.

II SKYRIUS
UŽ FIZINĘ APSAUGĄ ATSAKINGO DARBUOTOJO FUNKCIJOS IR ATSAKOMYBĖS

8. Už fizinę apsaugą atsakingas asmuo atlieka šias funkcijos:

8.1. atsako už fizinio saugumo priemonių įgyvendinimą ir priežiūrą;

8.2. vykdo darbo kabinetų (patalpų) raktų (elektroninių ar fizinių) išdavimą ir apskaitą raktų išdavimo apskaitos žurnale (2 priedas);

8.3. užtikrina, kad šis Aprašas atitiktų galiojančius teisės aktus, standartus ir valstybinės archyvų sistemos įstaigų vidaus politiką;

8.4. pagal kompetenciją užtikrina tinkamą fizinio saugumo priemonių funkcionavimą ir techninę priežiūrą;

8.5. organizuoja darbuotojų mokymus apie fizinės saugos reikalavimus, įskaitant saugaus elgesio procedūras;

8.6. pagal savo kompetencijas dalyvauja darbo grupėse ir su fiziniu saugumu susijusiuose procesuose;

8.7. periodiškai, bent kartą per metus, atlieka fizinio saugumo priemonių profilaktinį patikrinimą, įvertindamas visų įstaigos įdiegtų fizinių ir technologinių saugumo priemonių būklę ir efektyvumą (spynų, vartų, seifų ir kitų užrakinimo mechanizmų veikimo patikrinimas, vaizdo stebėjimo kamerų, signalizacijos, judesio detektorių ir kitų elektroninių sistemų testavimas, dokumentų smulkintuvų, apsauginių pertvarų, fizinių barjerų ir įrangos tvirtinimo priemonių apžiūra). Tikrinimo tikslas – laiku nustatyti nusidėvėjusias, sugadintas ar neveikiančias priemones, įvertinti jų atitikimą pasikeitusiems saugumo reikalavimams bei užtikrinti nuolatinį efektyvų jų veikimą;

8.8. po įvykdytų patikrinimų arba pagal poreikį teikia ataskaitas su rekomendacijomis valstybinės archyvų sistemos įstaigos vadovui dėl esamos fizinės apsaugos situacijos ir papildomų fizinio saugumo priemonių įdiegimo ar esamų priemonių tobulinimo;

8.9. įvykus incidentui, susijusiam su fizine apsauga, koordinuoja veiksmus incidentui suvaldyti ir užtikrina greitą jų sprendimą;

8.10. bendradarbiauja su teisėsaugos ar kitomis išorinėmis institucijomis, jei to reikalauja incidentas, susijęs su fizine apsauga;

8.11. užtikrina, kad visi incidentai, susiję su fizine apsauga, būtų tinkamai registruojami, tiriami ir analizuojami, o išvados būtų taikomos fizinio saugumo priemonių tobulinimui;

8.12. saugo visą informaciją apie incidentus, susijusius su fizine apsauga.

III SKYRIUS
PATALPOMS KELIAMI REIKALAVIMAI

9. Valstybinės archyvų sistemos įstaigų naudojamos patalpos skirstomos į šias kategorijas:

9.1. A – specialiosios paskirties patalpos (TIS serverių patalpos, patalpos, kuriose saugomos atsarginės duomenų kopijos ir kitos patalpos, kurioms reikalingas aukščiausias saugumo lygis);

9.2. B – darbo vietų (darbinės) patalpos (patalpos į kurias gali patekti tik valstybinės archyvų sistemos įstaigų darbuotojai, kuriems nustatyta tvarka yra suteikti leidimai patekti į teritoriją);

9.3. C – patalpos (patalpos, į kurias gali patekti tretieji asmenys, nedirbantys valstybinės archyvų sistemos įstaigose).

10. Specialiosios paskirties patalpos registruojamos Reikalingų apsaugoti patalpų sąraše (3 priedas), kuris yra tvirtinimas kartu su šiuo Aprašu. Šis sąrašas yra laikomas konfidencialia informacija.

11. Tais atvejais, kai specialiosios paskirties patalpos sutampa su kitų kategorijų patalpomis, taikomi griežtesni šių patalpų saugumo reikalavimai.

12. Reikalavimai specialiosios paskirties patalpų fizinei apsaugai (A kategorija):

12.1. patalpos turi būti apsaugotos nuo neteisėto asmenų patekimo į jas, taikant atitinkamas fizinio saugumo priemones;

12.2. ant visų prieigų į patalpas matomoje vietoje turi būti draudžiamieji ženklai, kuriuose aiškiai ir suprantamai matytųsi draudimas patekti į patalpas tam leidimo neturintiems asmenims;

12.3. prieiga prie šių patalpų suteikiama tik įgaliotiems darbuotojams, kurie yra įtraukti į reikalingų apsaugoti patalpų sąrašą kaip už šias patalpas atsakingi darbuotojai arba kurių tiesioginės darbo funkcijos yra susijusios su TIS įrangos šiose patalpose priežiūra;

12.4. į patalpas gali patekti tik asmenys, kurių darbo funkcijos susijusios su toje patalpoje esančia įrangos kontrole, visi kiti asmenys į patalpas gali patekti tik lydimi atsakingo darbuotojo;

12.5. asmenų patekimas į patalpas turi būti kontroliuojamas, užrakinant duris fiziniais raktais arba naudojant elektroninę įeigos kontrolės sistemą;

12.6. bet koks apsilankymas šiose patalpose turi būti registruojamas Įėjimo į specialiosios paskirties patalpas kontrolės žurnale (4 priedas);

12.7. numatytos procedūros, kaip elgtis įvykus avarinei situacijai (pvz., gaisrui, patalpų užliejimu vandeniu, ar kitai panašu poveikį galinčiai turėti situacijai), siekiant apsaugoti svarbius įrenginius, turtą ir duomenis. Šios ir kitos potencialios situacijos turi būti aprašytos Veiklos tęstinumo valdymo plane;

12.8. patalpos turi būti be langų, o jei langai yra, jie turi būti neatidaromi ir apsaugoti fizinėmis barjerinėmis priemonėmis (pvz., grotomis, apsauginėmis žaliuzėmis) ir

(arba) apsauginėmis plėvelėmis, ir šis atvejis turi būti suderintas su Kibernetinio saugumo vadovu;

12.9. patalpų sienos, lubos ir grindys turi būti tvirtos konstrukcijos, užtikrinančios atsparumą fiziniam įsilaužimu;

12.10. patalpose turi būti įrengtos arba prieinamos gaisro gesinimo priemonės, pritaikytos elektros ir elektroninei įrangai gesinti;

12.11. patalpose turi būti įrengta perspėjimo nuo įsilaužimo patalpas signalizacija, kurios galinė įranga turi būti suvesta į patalpą, kurioje vykdomas budėjimas, arba į apsaugos tarnybos stebėjimo pultą;

12.12. jei TIS serverių patalpose esančios įrangos bendras galingumas yra daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga, užtikrinanti tinkamą aplinkos temperatūrą ir drėgnumą;

12.13. jei šiose patalpose naudojama TIS kompiuterinė įranga, patalpoje turi būti įtampos filtras ir nepertraukiamo maitinimo šaltinis, užtikrinantis techninės įrangos veikimą;

12.14. kritiniai elementai (oro kondicionavimo įranga, vėdinimas ir drėgmės kontrolė, el. energijos tiekimas) turi būti dubliuojami, siekiant užtikrinti aukštą patalpoms eksploatuoti būtinų įrenginių patikimumą.

13. Reikalavimai darbo vietų patalpų fizinei apsaugai (B kategorija):

13.1. prieiga prie darbo vietų patalpų suteikiama tik darbuotojams, kurie pagal einamas pareigas dirba arba vykdo užduotis šiose patalpose, arba asmenims, dirbantiems paslaugas teikiančiose įmonėse, su kuriomis valstybinė archyvų sistemos įstaiga yra pasirašiusi paslaugų teikimo sutartį;

13.2. patekimas į patalpas turi būti kontroliuojamas, užrakinant duris fiziniais raktais arba naudojant elektroninę įeigos kontrolės sistemą;

13.3. patalpose turi būti įrengta perspėjimo nuo įsilaužimo patalpas signalizacija, valdoma iš patalpos, kurioje vykdomas budėjimas, arba iš apsaugos tarnybos stebėjimo pulto;

13.4. lankytojai į patalpą gali patekti tik su jiems išduota svečio kortele, lydim atsakingo asmens. Išėjus iš patalpų svečio kortelė grąžinama budėtojui.

14. Reikalavimai viešai prieinamų patalpų fizinei apsaugai (C kategorija):

14.1. į patalpas gali laisvai patekti visi lankytojai valstybinės archyvų sistemos įstaigos darbo valandomis;

14.2. pagal poreikį patekimo į patalpas prieigos gali būti filmuojamos, o patalpose gali būti įrengtos vaizdo stebėjimo kameros, skirtos užtikrinti viešajai tvarkai ir fiksuoti galimus incidentus.

15. Ne darbo valandomis visų valstybinės archyvų sistemos įstaigų pastatų durys turi būti užrakintos.

16. Visose patalpose turi būti įrengta gaisrinė signalizacija, sujungta su pastato apsaugos sistema.

17. Darbo vietų patalpos gali būti stebimos vaizdo kameromis.

18. Raktai nuo patalpų turi būti apskaitomi ir darbuotojams išduodami pasirašytinai.

19. Elektros maitinimo ir ryšių kabeliai, vedami į pastatus, kuriuose yra valstybinės archyvų sistemos įstaigų patalpos ar įranga, turi būti įrengti rakinamoje patalpoje ir apsaugoti nuo neleistinos prieigos. Raktus (pagrindinį ir atsarginį komplektus) saugo ir naudoja fizinės saugos įgaliotinis.

IV SKYRIUS
DARBUOTOJŲ ĮSIPAREIGOJIMAI

20. Darbuotojai turi susipažinti su šiuo Aprašu, kad užtikrintų patalpų fizinės apsaugos reikalavimus.

21. Darbuotojai, pastebėję incidentų, susijusių su fizine apsauga, turi apie tai nedelsiant pranešti fizinės saugos įgaliotiniui. Ekstremalių įvykių atvejais darbuotojai turi laikytis sudarytų evakuacijos planų.

22. B kategorijos patalpose darbuotojai, pasitraukdami iš darbo vietos, privalo laikytis „švaraus stalo" politikos.

23. Darbuotojas, pastebėjęs, kad į darbines patalpas nesankcionuotai (be leidimo) pateko neturintys teisės to daryti darbuotojai ar tretieji asmenys, apie tai nedelsdamas žodžiu, telefonu ir (ar) raštu informuoja už fizinę apsaugą atsakingą darbuotoją ar budėtoją.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

24. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba atsiradus esminių pokyčių, galinčių turėti įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas Kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

_____

Fizinės apsaugos tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

FIZINĖS APSAUGOS TVARKOS PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	Statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Fizinės apsaugos tvarkos aprašo
2 priedas

(Raktų išdavimo apskaitos žurnalo forma)

RAKTŲ IŠDAVIMO APSKAITOS ŽURNALAS

Eil. Nr.	Darbuotojo vardas, pavardė	Kabineto (patalpos) numeris (pavadinimas)	Išdavimo laikas	Paėmusio asmens parašas	Grąžinimo laikas	Priėmusio asmens parašas	Pastabos

_____

Fizinės apsaugos tvarkos aprašo
3 priedas

(Reikalingų apsaugoti patalpų sąrašo forma)

REIKALINGŲ APSAUGOTI PATALPŲ SĄRAŠAS

Eil. Nr.	Patalpos paskirtis	Patalpos numeris	Patalpos kategorija	Atsakingas darbuotojas	Pastabos

_____

Fizinės apsaugos tvarkos aprašo
4 priedas

(Įėjimo į specialios paskirties patalpas kontrolės žurnalo forma)

ĮĖJIMO Į SPECIALIOS PASKIRTIES PATALPAS KONTROLĖS ŽURNALAS

Eil. Nr.	Data	Asmens vardas, pavardė	Apsilankymo tikslas	Patalpos pavadinimas (numeris)	Įėjimo laikas	Lankytojo parašas

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

PRIEIGŲ VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Prieigų valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja naudotojų paskyrų sukūrimo, keitimo, stabdymo ir naikinimo bei prieigos prie Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) tinklų ir informacinių sistemų suteikimo, keitimo, sustabdymo ir naikinimo bei kontrolės užtikrinimo, taip pat slaptažodžių valdymo ir kontrolės užtikrinimo procesą.

2. Apraše vartojamos sąvokos:

2.1. **Informacinių technologijų pagalbos tarnyba** (angl. *Service desk*) (toliau – IT pagalbos tarnyba) – valstybinės archyvų sistemos įstaigų naudojama informacinė sistema ar programinė įranga informacinių technologijų kreipiniams ir problemoms bei kibernetinio saugumo įvykiams ir incidentams, taip pat pokyčiams registruoti ir valdyti; Nesant IT pagalbos tarnybos, prašymai suteikti, pakeisti, sustabdyti arba panaikinti paskyrą ir prieigos teises gali būti teikiami elektroniniu paštu už IT priežiūrą atsakingam padaliniui arba darbuotojui (TIS administratoriui);

2.2. **Kibernetinio saugumo vadovas** – asmuo, atsakingas už kibernetinio saugumo subjekto atitikties Lietuvos Respublikos kibernetinio saugumo įstatymo 14 ir 18 straipsniuose nustatytiems reikalavimams įgyvendinimą ir atliekantis kitas kibernetinį saugumą reglamentuojančiuose teisės aktuose nustatytas funkcijas;

2.3. **Naudotojas** – valstybinės archyvų sistemos įstaigos darbuotojas ar trečiosios šalies atstovas, turintis paskyrą ir (ar) prieigą prie valstybinės archyvų sistemos įstaigos tinklų ir informacinių sistemų. **Standartinis naudotojas** turi standartines teises prisijungti ir naudotis valstybinės archyvų sistemos įstaigos tinklų ir informacine sistema, bet negali atlikti jokių sisteminių ar kitų tinklų ir informacinių sistemų pokyčių, konfigūracijų ar programinės įrangos diegimų. **Privilegijuotam naudotojui** suteikiamos teisės atlikti kai kurias tinklų ir informacinių sistemų administravimo funkcijas (privilegijuoti naudotojai dažniausiai yra valstybinės archyvų sistemos įstaigos ar tiekėjo tinklų ir informacinių sistemų palaikymo funkcijas vykdantys darbuotojai, turintys papildomas teises, pvz. teisę prisijungti prie serverių, aptarnauti duomenų bazes ir pan.);

2.4. **PAM** sprendimas (Privilegijuotų prieigų valdymo, angl. *Privileged Access Managemen*t) – sprendimas, skirtas centralizuotai valdyti, stebėti ir audituoti privilegijuotų paskyrų naudojimą;

2.5. **Paskyra** – unikalus identifikatorius, suteikiantis naudotojui ar techninei sistemai prieigą prie tinklų ir informacinių sistemų;

2.6. **Paskyrų valdymas** – tinklų ir informacinių sistemų naudotojų paskyrų sukūrimas, keitimas, sustabdymas ar naikinimas ir kontrolės užtikrinimas;

2.7. **Perėjimo serveris** (angl. *Jump Host / Jump Server*) – specialiai

sukonfigūruotas, itin apsaugotas tarpinis serveris arba tinklo mazgas, per kurį privaloma jungtis, norint pasiekti kritinius TIS komponentus (serverius, duomenų bazes, tinklo įrangą). Perėjimo serveris neturi turėti prieigos prie interneto.

2.8. **Prieiga** – galimybė naudotis tinklų ir informacinėmis sistemomis, atsižvelgiant į suteiktas teises (teisių rinkinį);

2.9. **Prieigos užsakovas** – valstybinės archyvų sistemos įstaigos darbuotojas arba jo vadovas (arba už sutartį su trečiąja šalimi atsakingas valstybinės archyvų sistemos įstaigos darbuotojas) už IT priežiūrą atsakingam padaliniui arba darbuotojui (TIS administratoriui) teikiantis prašymą suteikti, pakeisti, sustabdyti arba panaikinti paskyrą ir prieigos teises prie valstybinės archyvų sistemos įstaigos tinklų ir informacinių sistemų;

2.10. **Prieigų valdymas** – prieigos teisių (teisių rinkinių) prie valstybinės archyvų sistemos įstaigos tinklų ir informacinių sistemų suteikimas, keitimas, sustabdymas ar naikinimas tinklų ir informacinių sistemų naudotojams ir kontrolės užtikrinimas;

2.11. **Sisteminė paskyra** – techninė paskyra, naudojama tinklų ir informacinėje sistemoje aplikacijos ar automatizuotų procesų veikimui užtikrinti;

2.12.**Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

2.13.**Tinklų ir informacinių sistemų administratorius** (toliau – IT administratorius) – valstybinės archyvų sistemos įstaigos darbuotojas arba padalinys, atliekantis TIS priežiūrą, kuris yra atsakingas už naujų tinklų ir informacinių paskyrų sukūrimą, sustabdymą ar panaikinimą bei prieigų prie valstybinės archyvų sistemos įstaigos tinklų ir informacinių sistemų suteikimą, keitimą, sustabdymą ar panaikinimą pagal Prieigos užsakovo pateiktą prašymą ir tinklų ir informacinių sistemų savininko nurodymą.

3. Pagrindiniai valstybinės archyvų sistemos įstaigų paskyrų ir prieigos teisių valdymo principai:

3.1. Būtina žinoti (angl. *Need to know*) – standartiniams ir privilegijuotiems naudotojams turėtų būti suteikta prieiga tik prie tų sistemos tvarkomų duomenų, kurie reikalingi jų darbo funkcijoms atlikti ar sutartiniams įsipareigojimams įgyvendinti;

3.2. Mažiausios privilegijos (angl. *Least privilege*) – naudotojams suteikiamos mažiausios prieigos teisės prie sistemos tinklų ir informacinių sistemų, reikalingų jų darbo funkcijoms atlikti ar sutartiniams įsipareigojimams įgyvendinti, bet ne daugiau;

3.3. Pareigų atskyrimas (angl. *Segregation of duties*) – valstybinės archyvų sistemos įstaigose turi būti sukurtos procedūros ir organizacinė struktūra, kurios neleistų vienam naudotojui kontroliuoti visų pagrindinių tinklų ir informacinių sistemų veiklos aspektų, atlikti neleistinus veiksmus ar neteisėtai pasiekti organizacijos tinklų ir informacines sistemas ir juose esančius duomenis.

4. Valstybinės archyvų sistemos įstaigos privalo įgyvendinti Kibernetinio saugumo įstatymą ir Kibernetinio saugumo reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 3 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“, numatytus techninius prieigos valdymo ir

tapatumo nustatymo reikalavimus, kurie pateikti šiame Apraše.

II SKYRIUS
ATSAKINGŲ DARBUOTOJŲ FUNKCIJOS IR ATSAKOMYBĖS

5. Kibernetinio saugumo vadovo funkcijos ir atsakomybės:

5.1. užtikrina, kad valstybinės archyvų sistemos įstaigose būtų visa apimtimi įgyvendinti šiame Apraše numatyti prieigos valdymo ir tapatumo nustatymo reikalavimai;

5.2. užtikrina, kad naudotojų paskyrų ir prieigos prie TIS valdymo procesai būtų įgyvendinami pagal šio Aprašo reikalavimus;

5.3. rengia ir esant poreikiui koreguoja paskyrų ir prieigų matricą pagal šio Aprašo 2 priede pateiktą Paskyrų ir prieigų prie TIS matricos formą;

5.4. vertina periodinių prieigų valdymo auditų rezultatus;

5.5. bent kartą per metus arba atsiradus esminių pokyčių, galinčių turėti įtakos šiam Aprašui, peržiūri ir atnaujina šį Aprašą;

5.6. pildo ir laiku atnaujina TIS administratorių sąrašą pagal šio Aprašo 4 priede pateiktą Tinklų ir informacinių sistemų administratorių sąrašo formą;

5.7. TIS turto valdymo apraše numatytos Konfidencialios informacijos valdymo pagrindu užtikrina TIS administratorių sąrašo apsaugą;

5.8. atlieka periodines ir neplanuotas TIS administratorių paskyrų ir (ar) prieigų peržiūras ir auditus;

5.9. teikia privalomus nurodymus naudotojams ir TIS administratoriams, siekiant užtikrinti tinkamą paskyrų ir prieigų valdymą.

6. Prieigos užsakovo funkcijos ir atsakomybės:

6.1. teikia prašymus sukurti, pakeisti, sustabdyti ir panaikinti paskyras naudotojams, vadovaudamasis paskyrų ir prieigos teisių valdymo principais;

6.2. teikia prašymus suteikti, pakeisti, sustabdyti ar panaikinti prieigas prie TIS naudotojams, vadovaudamasis paskyrų ir prieigos teisių valdymo principais;

6.3. užtikrina, kad TIS administratorius laiku gautų prašymą ir laiku sukurtų, sustabdytų, panaikintų paskyras ar suteiktų, pakeistų, sustabdytų, panaikintų prieigas prie TIS.

7. TIS administratoriaus funkcijos ir atsakomybės:

7.1. pildo ir laiku atnaujina Paskyrų ir prieigos teisių valdymo registrą pagal šio Aprašo 3 priede numatytą Paskyrų ir prieigos teisių valdymo registro formą;

7.2. kuria, stabdo ir naikina naudotojų paskyras ir prieigas prie TIS;

7.3. pagal kompetenciją įgyvendina Mažiausios privilegijos principą;

7.4. jei yra techninės galimybės konkrečioje TIS, kartu su naudotojų paskyromis įgalina dviejų faktorių autentifikavimo (angl. *two-factor authentication*) naudojimą;

7.5. jei organizacija turi privilegijuotų naudotojų valdymo sprendimą (angl. *Privileged Access Management*, toliau – PAM sprendimas), administruoja šį sprendimą;

7.6. įgyvendina periodinę naudotojų prieigų ir teisių peržiūrą;

7.7. užtikrina, kad TIS administratoriaus funkcijos būtų atliekamos naudojant atskirą tam skirtą paskyrą, kuri negali būti naudojama kasdienėms naudotojo funkcijoms atlikti;

7.8. TIS administratoriaus paskyras ir prieigas prie TIS naudoja išskirtinai TIS administratoriaus funkcijoms vykdyti;

8. TIS naudotojų funkcijos ir atsakomybės:

8.1. naudoja paskyras ir prieigas prie TIS tik pavestoms funkcijoms vykdyti;

8.2. neleidžia naudotis paskyromis ir prieigomis prie TIS kitiems su jam pavestų funkcijų įgyvendinimu nesusijusiems asmenims;

8.3. vykdo TIS administratorių ir kibernetinio saugumo vadovo nurodymus, susijusius su paskyrų, prieigų ir slaptažodžių valdymu.

III SKYRIUS
PASKYRŲ IR PRIEIGŲ VALDYMAS

9. Užtikrinant paskyrų ir prieigų valdymą, turi būti įgyvendinti visi šiame Apraše nustatyti paskyrų ir prieigų valdymo reikalavimai. Visos – tiek centralizuotai valdomos, tiek lokalios – naudotojų ir TIS administratorių paskyros privalo griežtai atitikti šiame Apraše nustatytus tapatybės patvirtinimo ir prieigos kontrolės reikalavimus.

10. Kibernetinio saugumo vadovas, atsižvelgdamas į organizacinę ir funkcinę struktūrą bei valdomas TIS, turi sudaryti paskyrų ir prieigų matricą pagal šio Aprašo 2 priede pateiktą Paskyrų ir prieigų prie Tinklų ir informacinių sistemų matricos formą (toliau – Paskyrų ir prieigų matrica), kurioje pagal sudarytas TIS naudotojų ir TIS administratorių grupes nustatoma paskyrų ir prieigų prie TIS tvirtinimo tvarka. Sudarant Paskyrų ir prieigų matricą privaloma numatyti, kurias privilegijuotas paskyras ir suteikiamas prieigas prie TIS turi papildomai patvirtinti kibernetinio saugumo vadovo paskirti atsakingi asmenys.

11. Naujos paskyros sukūrimo ir prieigos prie TIS suteikimo procesas:

11.1. Nauja TIS naudotojo paskyra sukuriama priėmus į darbą naują darbuotoją, esamą darbuotoją perkėlus į kitas pareigas, kurių funkcijoms atlikti būtinos prieigos teisės, arba sudarius paslaugos teikimo sutartį su trečiąja šalimi (pvz. su TIS priežiūros ir vystymo paslaugas teikiančiu tiekėju), jei paslauga negali būti suteikta be paskyros ir prieigos prie TIS sukūrimo ir suteikimo;

11.2. Esant bent vienai iš aukščiau numatytų aplinkybių, prieigos užsakovas TIS administratoriui elektroniniu paštu per IT pagalbos tarnybą pateikia prašymą sukurti paskyrą ar suteikti prieigą prie TIS. Prašyme nurodoma:

11.2.1. darbuotojo (trečiosios šalies darbuotojo), kuriam reikia sukurti paskyrą ar prieigą prie TIS, vardas, pavardė, padalinys ir pareigos;

11.2.2. naujos paskyros sukūrimo priežastis;

11.2.3. paskyros tipas;

11.2.4. reikalingų suteikti prieigų prie TIS teisių sąrašas (teisių rinkinys);

11.2.5. paskyros ir (ar) prieigos apribojimai, jei tokių yra;

11.2.6. paskyros aktyvavimo data. Naujai sukurta paskyra gali būti aktyvuojama ne anksčiau kaip pirmą darbuotojo darbo dieną. Trečiosios šalies darbuotojo paskyra aktyvuojama ne anksčiau nei pradeda galioti pasirašyta sutartis. Išimtis gali būti taikoma tik tais atvejais, kai sudaromoje sutartyje nurodomos kitos datos.

11.3. Prieigos užsakovas prašymus turi teikti vadovaudamasis paskyrų ir prieigos

teisių valdymo principais.

11.4. TIS administratorius, gavęs prašymą sukurti naują naudotojo paskyrą ir jam suteikti prieigą prie TIS, turi užtikrinti, kad būtų įgyvendintos priemonės TIS naudotojo tapatybei nustatyti.

11.5. Prašymą sukurti paskyrą ir suteikti prieiga privilegijuotam naudotojui ar sisteminei paskyrai papildomai turi patvirtinti paskirtas atsakingas darbuotojas pagal Paskyrų ir prieigų matricą.

11.6. Prašymą sukurti paskyrą TIS administratoriui ir jam suteikti prieigą prie TIS papildomai turi patvirtinti kibernetinio saugumo vadovas.

12. Darbuotojams, vykdantiems specifines su TIS administravimu susijusias funkcijas (pvz. vykdantiems TIS priežiūrą ir vystymą, suteikiantiems prieigas standartiniams naudotojams ir pan.), kartu su privilegijuota ir (ar) TIS administratorius paskyra turi būti sukurta ir standartinio naudotojo paskyra kasdienėms funkcijos vykdyti ir jai suteiktos prieigos prie TIS.

13. Privilegijuotiems naudotojams ir TIS administratoriams draudžiama naudoti privilegijuotas ar TIS administratoriaus paskyras, jei atliekami darbai ar funkcijos nereikalauja privilegijuotų prieigos teisių.

14. Galiojančios paskyros ir jai suteiktų prieigų keitimas yra įgyvendinamas tokia pačia tvarka kaip ir naujos paskyros sukūrimas ir prieigų suteikimas. Atsiradus poreikiui pakeisti paskyrą ir (ar) prieigas (pvz., pasikeitus darbuotojo funkcijoms arba keičiant TIS priežiūros ir plėtojimo paslaugų sutartį), prieigos užsakovas teikiamame prašyme papildomai turi nurodyti, ar darbuotojo naudojama paskyra turi būti palikta, ar ją reikia panaikinti, ar naudotojui suteiktos prieigos turi būti paliktos, bei nurodyti terminą, nuo kada turi būti įgyvendintas pakeitimas.

15. Paskyros ir prieigos prie TIS sustabymo (angl. *deactivation*) procesas:

15.1. atsiradus poreikiui (pvz., darbuotojo motinystės ar tėvystės atostogų metu, sustabdžius paslaugos teikimo sutartį, įvykus kibernetiniam incidentui, laiku tinkamai neįdiegus programinės įrangos atnaujinimo ar kitais atvejais) prieigos užsakovas TIS administratoriui elektroniniu paštu per IT pagalbos tarnybą pateikia prašymą sustabdyti paskyrą ar prieigą prie TIS. Prašyme nurodoma:

15.1.1. darbuotojo (trečiosios šalies darbuotojo), kurio paskyrą ir (ar) prieigas prie TIS reikia sustabdyti, vardas, pavardė, padalinys ir pareigos;

15.1.2. prieigos sustabdymo priežastis;

15.1.3. data, nuo kada paskyra ar prieiga turi būti sustabdyta;

15.1.4. jei žinoma, – data, nuo kada paskyra ar prieiga vėl turi būti aktyvuota.

15.2. TIS administratorius, gavęs prašymą sustabdyti naudotojo paskyrą ir (ar) jam suteiktas prieigas prie TIS, vadovaujasi prašyme pateikta informacija ir jame nurodytais terminais.

15.3. Kibernetinio saugumo vadovo pavedimu TIS administratorius bet kurią naudotojo paskyrą ir (ar) prieigą turi sustabdyti nurodytais terminais.

16. Paskyros ir prieigos prie TIS panaikinimo procesas:

16.1. pasibaigus darbuotojo darbo santykiams arba pasibaigus TIS priežiūros ir plėtojimo paslaugų teikimo sutarčiai ar sutartį nutraukus, prieigos užsakovas TIS

administratoriui elektroniniu paštu per IT pagalbos tarnybą pateikia prašymą panaikinti paskyrą ar prieigą prie TIS. Prašyme nurodoma:

16.1.1. darbuotojo (trečiosios šalies darbuotojo), kurio paskyrą ir (ar) prieigas prie TIS reikia panaikinti, vardas, pavardė, padalinys ir pareigos;

16.1.2. panaikinimo priežastis;

16.1.3. data (imtinai), nuo kada paskyra turi būti panaikinta.

16.2. Šio Aprašo 15 punkte nurodytais atvejais sustabdytos paskyros turi būti automatiškai naikinamos po 3 mėnesių nuo jų sustabdymo dienos.

17. TIS administratoriams prisijungiant prie kritinių TIS komponentų (pvz., serverių, tinklo įrangos, duomenų bazių), draudžiama jungtis tiesiogiai iš naudotojo darbo vietos. Tokie prisijungimai privalo būti vykdomi tik per tarpinį perėjimo serverį (angl. *Jump Host*) arba naudojant centralizuotą privilegijuotų prieigų valdymo (PAM) sprendimą, naudojant kriptografinius SSH autentifikavimo raktus pagal šio Aprašo 44 punkto reikalavimus.

18. Visa informacija apie paskyrų ir prieigų prie TIS valdymą tą pačią dieną, kai įvyko su paskyrų ar prieigų valdymu susijęs veiksmas, turi būti registruojama Paskyrų ir prieigos teisių valdymo registre, rengiamame pagal šio Aprašo 3 priede pateiktą Paskyrų ir prieigos teisių valdymo registro formą. Už Paskyrų ir prieigos teisių valdymo registro pildymą ir atnaujinimą yra atsakingas TIS administratorius.

19. Kiekvienas naudotojas TIS turi būti unikaliai atpažįstamas.

20. Naudotojas ir TIS administratorius turi patvirtinti savo tapatybę slaptažodžiu ir papildoma tapatumo nustatymo priemone (kelių veiksnių autentifikavimas).

21. TIS turi būti sukonfigūruota taip, kad po ne daugiau kaip 5 iš eilės nesėkmingų prisijungimo bandymų naudotojo paskyra būtų automatiškai užblokuojama. Paskyros atblokavimą gali atlikti tik įgalioti TIS administratoriai.

22. Naudotojo teisė dirbti su konkrečia TIS turi būti automatiškai sustabdoma, kai naudotojas nesinaudoja TIS ilgiau kaip 3 mėnesius. TIS administratoriaus teisė dirbti su TIS turi būti sustabdoma, kai TIS administratorius nesinaudoja TIS ilgiau kaip 2 mėnesius.

23. Kai naudotojas ar TIS administratorius nušalinamas nuo darbo (pareigų), neatitinka kituose teisės aktuose nustatytų kvalifikacinių reikalavimų, pat pasibaigia jo darbo (tarnybos) santykiai arba jis praranda patikimumą, jo teisė naudotis TIS turi būti panaikinta tą pačią darbo dieną.

24. Nereikalingos ar nenaudojamos TIS paskyros turi būti blokuojamos per organizacijos nustatytą terminą ir ištrinamos praėjus žurnalinių įrašų saugojimo terminui (ne trumpiau kaip 90 kalendorinių dienų).

IV SKYRIUS
DARBO VIETOS SAUGUMAS

25. Naudotojas, baigęs darbą arba pasitraukdamas iš darbo vietos, privalo atsijungti nuo TIS ir įjungti ekrano užsklandą su slaptažodžiu.

26. TIS darbo stotis turi būti sukonfigūruota taip, kad neatliekant jokių veiksmų ne ilgiau kaip po 15 minučių darbo stotis automatiškai užsirakintų ir toliau naudotis TIS būtų galima tik pakartotinai patvirtinus savo tapatybę.

27. TIS dalys, tarp jų svetainės ir naršyklės, patvirtinančios naudotojo tapatumą,

turi drausti išsaugoti slaptažodžius, išskyrus specializuotą slaptažodžių tvarkymo programinę įrangą (angl. *password vault)*.

V SKYRIUS
PASKYRŲ IR PRIEIGOS TEISIŲ PERŽIŪRA IR ATITIKTIES REIKALAVIMAI

28. Naudotojų paskyros ir prieigos prie TIS turi būti peržiūrimos periodiškai, ne rečiau kaip kartą per ketvirtį, siekiant užtikrinti, kad visų naudotojų paskyros ir prieigos teisės būtų sustabdytos ar panaikintos, pasibaigus poreikiui. Už paskyrų ir prieigos teisių peržiūrą atsakingas TIS administratorius ir (ar) paslaugų teikėjo atsakingas darbuotojas (jei paskyras ir (ar) prieigas sutarties pagrindu valdo trečioji šalis).

29. TIS administratorius, atlikęs paskyrų ir prieigos teisių peržiūrą, informaciją apie tai fiksuoja Paskyrų ir prieigos teisių valdymo registre ir papildomai pateikia kibernetinio saugumo vadovui.

30. TIS administratorius (arba trečiosios šalies atstovas, jei paskyras ir (ar) prieigas sutarties pagrindu valdo trečioji šalis), nustatęs, kad paskyros ir prieigos yra valdomos ne pagal šį Aprašą, turi nedelsiant ištaisyti neatitikimus ir apie tai informuoti kibernetinio saugumo vadovą.

31. TIS administratorius yra atsakingas, kad būtų tinkamai užpildytas ir laiku atnaujintas Paskyrų ir prieigos teisių valdymo registras.

VI SKYRIUS
PRIVILEGIJUOTŲ NAUDOTOJŲ VYKDOMŲ VEIKSMŲ KONTROLĖS ĮGYVENDINIMAS

32. Valstybinės archyvų sistemos įstaigos turi įgyvendinti organizacines ir technines priemones, siekiant tinkamai užtikrinti privilegijuotų naudotojų vykdomų veiksmų kontrolę. Šiam tikslui gali būti sudarytas ir administruojamas privilegijuotų naudotojų sesijų valdymo registras, kuriame būtų fiksuojama informacija apie tai, kada (nurodant pradžios ir pabaigos datą), koks privilegijuotas naudotojas prie kurių TIS prisijungė, kokiu tikslu ir kokius veiksmus atliko.

VII SKYRIUS
TINKLŲ IR INFORMACINIŲ SISTEMŲ ADMINISTRATORIŲ KONTROLĖ

33. Kibernetinio saugumo vadovas turi sudaryti asmenų, kuriems suteiktos TIS administratoriaus teisės prisijungti prie TIS, sąrašą (toliau – TIS administratorių sąrašas), rengiamą pagal šio Aprašo 3 priede pateiktą Tinklų ir informacinių sistemų administratorių sąrašo formą. TIS administratorių sąraše kibernetinio saugumo vadovas turi suvesti informaciją apie TIS administratorius, jiems sukurtas, sustabdytas ir panaikintas paskyras ir suteiktas, sustabdytas ir panaikintas prieigas prie TIS. Kibernetinio saugumo vadovas TIS administratorių sąrašą turi peržiūrėti nedelsiant, kai TIS administratorius nušalinamas arba pasibaigia jo darbo (tarnybos) santykiai.

34. Kibernetinio saugumo vadovas ne rečiau kaip kartą per metus turi atlikti TIS administratorių paskyrų ir prieigų auditą ir įvertinti, ar TIS administratorių paskyros ir

prieigos prie TIS valdomos šiame Apraše nustatyta tvarka. Esant poreikiui, kibernetinio saugumo vadovas gali atlikti ir neeilinį TIS administratorių paskyrų ir (ar) prieigų auditą.

35. Kibernetinio saugumo vadovas informaciją apie atliktą TIS administratorių sąrašo peržiūrą ir (ar) TIS administratorių paskyrų ir teisių auditą turi suvesti į TIS administratorių sąrašą.

VIII SKYRIUS
SLAPTAŽODŽIŲ VALDYMO REIKALAVIMAI

36. TIS administratorius, užtikrindamas slaptažodžių valdymą, turi įgyvendinti tokius TIS naudotojų slaptažodžių sudarymo, galiojimo trukmės ir keitimo reikalavimus:

36.1. slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, gimimo data, šeimos narių vardai ir panašiai);

36.2. slaptažodis negali būti sudarytas iš pasikartojančių arba nuoseklių simbolių (pvz., „aaaaaaaaaaaa“ arba „0123456789“) ar įprastos klaviatūros sekos (pvz., „Qwerty“);

36.3. slaptažodis turi būti sudarytas iš didžiųjų ir mažųjų raidžių, skaičių ir specialiųjų simbolių;

36.4. slaptažodį turi sudaryti ne mažiau kaip 10 simbolių.

37. Papildomi naudotojų slaptažodžių galiojimo ir keitimo reikalavimai:

37.1. slaptažodis turi būti keičiamas ne rečiau kaip kas 6 mėnesius;

37.2. slaptažodžio negalima pakartoti – sistema turi atmesti ne mažiau kaip paskutinių 5 naudotų slaptažodžių pakartojimą.

38. Privilegijuotų naudotojų (TIS administratorių) paskyrų slaptažodžiams taikomi papildomi reikalavimai:

38.1. privilegijuoto naudotojo slaptažodį turi sudaryti ne mažiau kaip 15 simbolių;

38.2. privilegijuoto naudotojo slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius.

39. Sisteminėms paskyroms ir TIS programiniam kodui taikomi šie reikalavimai:

39.1. sisteminės paskyros slaptažodžiai turi būti unikalūs ir skirti tik konkrečiai paskyrai;

39.2. draudžiama naudoti numatytuosius (angl. *default*) gamintojo slaptažodžius sisteminėms paskyroms bei TIS techninėje ir programinėje įrangoje;

39.3. sisteminės paskyros slaptažodžiai keičiami ne rečiau kaip kartą per metus arba nedelsiant įvykus saugumo incidentui;

39.4. programiniame kode (angl. *hardcode)* draudžiama išsaugoti prisijungimo duomenis (vardą, slaptažodį, aplikacijų programavimo sąsajų (angl. API) raktus, prieigos žetonus (angl. Token) ir kt.), kuriuos atskleidus gali būti neteisėtai pasinaudota prieiga prie įrenginių, resursų, paskyrų ar TIS valdiklių.

40. Unikalų prisijungimo vardą ir pirminį slaptažodį darbuotojui ar trečiųjų šalių paslaugų teikėjui suteikia TIS administratorius, sukūręs paskyrą ir (ar) prieigas.

41. Prisijungimo vardą ir slaptažodį TIS administratorius naudotojui tiesiogiai perduoda konfidencialiai žodžiu arba kitomis saugiomis priemonėmis. TIS administratorius naudotojui laikiną slaptažodį gali perduoti atviru tekstu, tačiau atskirai nuo prisijungimo vardo, tik jeigu naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra

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

42. Naudotojų ir TIS administratorių nuotolinės prieigos prie TIS turi būti apsaugotos naudojant šifravimą ar virtualųjį privatų tinklą (angl. *Virtual private network,* VPN).

43. Naudotojams jungiantis prie kritinių, o TIS administratoriams jungiantis prie visų paskyrų ir (ar) TIS, turi būti naudojamos kelių veiksnių autentifikavimo (angl. *Multifactor Authentication*, *MFA*) priemonės, jeigu TIS palaiko tokį funkcionalumą.

44. Prisijungimui prie TIS komponentų per saugų nuotolinio prisijungimo protokolą (angl. *Secure Shell*, SSH) privaloma naudoti kriptografinius autentifikavimo raktus (angl. *SSH key pair*). Prisijungimas slaptažodžiu per SSH turi būti techniškai išjungtas, išskyrus atvejus, kai tai techniškai neįmanoma įgyvendinti konkrečioje TIS. Raktai turi atitikti Kriptografijos ir šifravimo naudojimo tvarkos aprašo reikalavimus.

45. Reikalavimai slaptažodžių saugojimui:

45.1. visi slaptažodžiai laikomi konfidencialia informacija ir negali būti atskleisti niekam, įskaitant, bet neapsiribojant, kitus darbuotojus, tiesioginį vadovą, valstybinės archyvų sistemos įstaigos vadovą, trečiąją šalį;

45.2. slaptažodžiai negali būti saugomi atviru tekstu ar užšifruojami nepatikimais algoritmais, išskyrus laikinuosius slaptažodžius, išduodamus pirmam naudotojo prisijungimui;

45.3. visi naudotojai yra atsakingi už savo prisijungimo duomenų slaptumą;

45.4. jei naudotojas įtaria, jog jo slaptažodis buvo atskleistas, jis apie tai privalo nedelsiant pranešti TIS administratoriui ir kibernetinio saugumo vadovui bei nedelsiant pasikeisti savo slaptažodį;

45.5. už slaptažodžių saugojimą, reguliarią peržiūrą, prieigos kontrolės užtikrinimą ir slaptažodžių valdymo proceso kontrolės įgyvendinimą yra atsakingas kibernetinio saugumo vadovas.

46. Darbuotojui draudžiama:

46.1. slaptažodžius siųsti elektroniniais laiškais (išskyrus pirminį slaptažodį, kurį reikia iš karto pasikeisti);

46.2. slaptažodžius atskleisti kitiems asmenims ir įvardyti telefoninio pokalbio metu;

46.3. nešifruotus slaptažodžius laikyti bet kur organizacijos patalpose (išskyrus seifą);

46.4. slaptažodžius saugoti elektronine forma bendruose TIS, jei jie yra nešifruoti.

47. TIS administratorių slaptažodžiai prie visų TIS gali būti saugomi centralizuotai, naudojant automatizuotą slaptažodžių valdymo sprendimą.

48. Rekomenduojama slaptažodžius saugoti šifruotoje saugykloje (angl. *password vault*).

IX SKYRIUS
DEBESŲ PASLAUGŲ PASKYRŲ VALDYMAS

49. Šio skyriaus nuostatos taikomos išorinių tiekėjų teikiamoms programinės įrangos kaip paslaugos (angl. *Software as a Service*, toliau – SaaS) platformoms (pvz., „Microsoft 365“). Tais atvejais, kai įstaiga debesijoje nuomojasi infrastruktūrą (virtualias mašinas), jose kuriamoms operacinių sistemų paskyroms taikomi standartiniai šio Aprašo III–VIII skyrių reikalavimai.

50. Debesų paslaugų paskyros, įskaitant išorinių naudotojų (svečių) paskyras, valdomos pagal šio Aprašo III skyrių, papildomai taikant šiuos reikalavimus:

50.1. kiekvienai naudojamai debesų ar SaaS paslaugai turi būti paskirtas atsakingas valstybinės archyvų sistemos įstaigos darbuotojas, užtikrinantis periodinę paskyrų ir prieigų peržiūrą;

50.2. suteikiant prieigą išoriniams naudotojams (svečiams), privaloma nurodyti tikslią prieigos galiojimo pabaigos datą, po kurios paskyra automatiškai sustabdoma. Visos paskyros registruojamos Paskyrų ir prieigos teisių valdymo registre;

50.3. visiems naudotojams privaloma įjungti kelių veiksnių autentifikavimą (MFA), jeigu SaaS paslauga palaiko tokį funkcionalumą; administracinė prieiga turi būti papildomai apsaugota sąlyginės prieigos (angl. Conditional Access) politikomis (pvz., ribojant prisijungimus pagal IP adresą ar naudojamą įrenginį);

50.4. vadovaujantis Mažiausios privilegijos principu, naudotojams suteikiamos tik jų funkcijoms atlikti būtinos specifinės rolės; draudžiama suteikti aukščiausio lygio (pvz., globalaus administratoriaus) teises, jeigu pakanka ribotesnės rolės.

51. Darbuotojui nutraukus darbo santykius, TIS administratorius jo debesų ir SaaS paslaugų paskyras, įskaitant prieigą prie elektroninio pašto ir debesijos failų saugyklų, panaikina arba blokuoja ne vėliau kaip paskutinę darbo dieną.

X SKYRIUS
BAIGIAMOSIOS NUOSTATOS

52. Visi organizacijos darbuotojai ir trečiosios šalys, turintys paskyras ir prieigą prie TIS, privalo laikytis šio Aprašo reikalavimų.

53. Kibernetinio saugumo vadovas užtikrina, kad naudotojų paskyrų valdymo bei prieigos prie TIS valdymo procesai būtų įgyvendinami pagal šio Aprašo reikalavimus.

54. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba atsiradus esminių pokyčių, galinčių turėti įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas. Aprašas peržiūrimas pagal 1 priede nustatytą apskaitos žurnalo formą.

_____

Prieigų valdymo aprašo
tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

PRIEIGŲ VALDYMO APRAŠO TVARKOS PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Prieigų valdymo aprašo
tvarkos aprašo
2 priedas

(Paskyrų ir prieigų prie Tinklų ir informacinių sistemų matricos forma)

PASKYRŲ IR PRIEIGŲ PRIE TINKLŲ IR INFORMACINIŲ SISTEMŲ MATRICA

Eil. Nr.	Naudotojų grupė	Paskyros tipas	Prieigų teisės	Prašymo tvirtintojas
1	*2*	*3*	*4*	*5*

[Pildymo instrukcija:
1. nurodomas eilės numeris;
2. nurodoma naudotojų grupė: (i) Organizacijos standartinis naudotojas; (ii) Tiekėjo standartinis naudotojas; (iii) Organizacijos privilegijuotas naudotojas; (iv) Tiekėjo privilegijuotas naudotojas; (v) Organizacijos TIS administratorius; (vi) Tiekėjo TIS administratorius;
3. nurodomas paskyros tipas: (i) standartinio naudotojo paskyra;(ii) privilegijuoto naudotojo paskyra; (iii) sisteminė paskyra;(iv) TIS administratoriaus paskira;
4. nurodomas naudotojui suteikiamų prieigų teisių (teisinių rinkinių) sąrašas, detalizuojant, prie kurių TIS yra suteiktos ir kokios prieigos ir jų teisės (teisių rinkiniai);
5. nurodomos prašymo tvirtintojo – organizacijos atsakingo darbuotojo, turinčio teisę patvirtinti paskyros sukūrimą ir (ar) prieigų suteikimą, pareigos, vardas ir pavardė.]

_____

Prieigų valdymo aprašo tvarkos aprašo
3 priedas

(Paskyrų ir prieigos teisių valdymo registro forma)

PASKYRŲ IR PRIEIGOS TEISIŲ VALDYMO REGISTRAS

Eil. Nr.	Paskyros naudotojas	Paskyros sukūrimo data	TIS administratorius	Paskyros tipas	Paskyros statusas	Paskyros sustabdymo/ panaikinimo data	Prieigų suteikimo data	Prieigų teisės	Prieigų statusas	Paskyros sustabdymo/ panaikinimo data	TIS administratorius	Peržiūros data	Peržiūros vykdytojas	Pastabos
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

[Pildymo instrukcija:

1. *nurodomas eilės numeris;*
2. *nurodomos paskyros naudotojo pareigos, vardas, pavardė;*
3. *nurodoma paskyros sukūrimo data;*
4. *nurodomos TIS administratoriaus, sukūrusio, sustabdžiusio ir panaikinusio paskyrą, pareigos, vardas ir pavardė;*
5. *nurodomas paskyros tipas: (i) standartinio naudotojo paskyra;(ii) privilegijuoto naudotojo paskyra; (iii) sisteminė paskyra;*
6. *nurodomas paskyros statusas: (i) sukurta, (ii) sustabdyta; (iii) panaikinta;*
7. *nurodoma paskyros sustabdymo ar panaikinimo data;*
8. *nurodoma prieigų suteikimo data;*
9. *nurodomas naudotojui suteiktų prieigų teisių (teisinių rinkinių) sąrašas, detalizuojant, prie kurių TIS yra suteiktos ir kokios prieigos ir jų teisės (teisių rinkiniai);*
10. *nurodomas prieigų statusas: (i)suteikta; (ii) sustabdyta; (iii) panaikinta;*
11. *nurodoma paskyros sustabdymo ar panaikinimo data;*
12. *nurodomos TIS administratoriaus, suteikusio, sustabdžiusio ir panaikinusio prieigas, pareigos, vardas ir pavardė;*
13. *nurodomos paskutinės peržiūros datos;*
14. *nurodomos paskutinę peržiūrą atlikusio darbuotojo pareigos, vardas ir pavardė;*
15. *pagal poreikį pateikiamos pastabos ir (ar) papildoma reikiama informacija].*

_____

Prieigų valdymo aprašo tvarkos aprašo
4 priedas

(Tinklų ir informacinių sistemų administratorių sąrašo forma)

TINKLŲ IR INFORMACINIŲ SISTEMŲ ADMINISTRATORIŲ SĄRAŠAS

Eil. Nr.	TIS administratorius	TIS administratoriaus darbovietė	TIS pavadinimas	Teisių lygis	Kibernetinio saugumo reikalavimai	Prieigos suteikimo data	Pavaduojantis TIS administratorius	Prieigos panaikinimo data	Audito data	Audito vykdytojas	Pastabos
1	2	3	4	5	6	7	8	9	10	11	12

[Pildymo instrukcija:

1. *nurodomas eilės numeris;*
2. *nurodomos TIS administratoriaus pareigos, vardas, pavardė;*
3. *nurodomos TIS administratoriaus darbovietė (tiekėjo atveju – tiekėjo pavadinimas);*
4. *nurodomas TIS, prie kurio TIS administratoriui suteikiama prieiga, pavadinimas;*
5. *nurodomi prieigos teisių lygiai (pvz. duomenų skaitymas, kūrimas, atnaujinimas, naikinimas, TIS naudotojų informacijos, prieigos teisių redagavimas ir panašiai);*
6. *nurodomi TIS administratoriams taikomi kibernetinio saugumo reikalavimai (pvz. nuotolinė prieiga tik naudojant mutifaktoriaus autentifikavimo priemones ir pan.)*
7. *nurodoma prieigos suteikimo data;*
8. *nurodomos pavaduojančio TIS administratoriaus pareigos, vardas, pavardė;*
9. *nurodoma prieigos panaikinimo data;*
10. *nurodoma paskutinio TIS administratorių prieigų audito data;*
11. *nurodomos paskutinio TIS administratorių prieigų auditą atlikusio darbuotojo pareigos, vardas, pavardė;*
12. *pagal poreikį pateikiamos pastabos ir (ar) papildoma reikiama informacija].*

_____

PATVIRTINTA
Lietuvos vyriausiojo archyvaro
įsakymu Nr.

TURTO VALDYMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Tinklų ir informacinių sistemų turto valdymo tvarkos aprašas (toliau – Aprašas) reglamentuoja Lietuvos vyriausiojo archyvaro tarnybos (toliau – LVAT) ir valstybės archyvų (toliau apibendrintai – valstybinės archyvų sistemos įstaiga (-os)) minimalius reikalavimus tinklų ir informacinių sistemų turto (toliau – Turtas) identifikavimui ir apskaitai, jo išdavimui ir gražinimui bei saugojimui (toliau – Turto valdymas), taip pat aprašo Turto valdymo procesą, siekiant užtikrinti, kad visas Turtas būtų unikaliai identifikuotas ir apskaitytas bei turėtų savininką.

2. Aprašas taikomas visam valstybinės archyvų sistemos įstaigų naudojamam Turtui ir visai jų valdomai ir tvarkomai informacijai.

3. Aprašo privalo laikytis visi valstybinės archyvų sistemos įstaigos darbuotojai, tvarkantys ir savo veikloje naudojantys Turtą bei tvarkantys ar valdantys informaciją.

4. Visa valstybinės archyvų sistemos įstaigų sukuriama ir naudojama informacija (žodinė, rašytinė ir elektroninė), esanti bet kokioje laikmenoje, yra klasifikuojama į viešąją informaciją ir konfidencialią informaciją, kuri nėra vieša.

5. Apraše vartojamos sąvokos:

5.1. **Asmens duomenys** – bet kokia informacija apie fizinį asmenį, kurio tapatybė nustatyta arba kurio tapatybę galima nustatyti tiesiogiai arba netiesiogiai pagal identifikatorių, vardą ir pavardę, asmens identifikavimo numerį, buvimo vietos duomenis ir interneto identifikatorių arba pagal vieną ar kelis to fizinio asmens fizinės, fiziologinės, genetinės, psichinės, ekonominės, kultūrinės ar socialinės tapatybės požymius. Šiame Apraše asmens duomenys yra viena konfidencialios informacijos rūšių;

5.2. **Darbuotojas** – valstybinės archyvų sistemos įstaigos valstybės tarnautojas arba darbuotojas, dirbantis pagal darbo sutartį (įskaitant studentą, organizacijoje atliekantį praktiką);

5.3. **Duomenų savininkas** – valstybinės archyvų sistemos įstaigos darbuotojas, kuriam priskiriama atsakomybė už duomenų valdymą ir (ar) tvarkymą;

5.4. **Informacija** – valstybinės archyvų sistemos įstaigos valdoma ir tvarkoma rašytinė ar elektroninė informacija ir duomenys, įskaitant asmens duomenis;

5.5. **Konfidenciali informacija** – valstybinės archyvų sistemos įstaigų disponuojama ir saugoma nevieša vertinga informacija, užfiksuota popierine ar elektronine forma, bei viešai neskelbtini asmens duomenys, kurių atskleidimas gali sukelti neigiamą poveikį organizacijai ar tretiesiems asmenims, įskaitant fizinius asmenis;

5.6. **Konfidencialumas** – tai sąlygų sudarymas, kad konfidenciali informacija būtų prieinama tik darbuotojams, kuriems yra suteikta tokia teisė, bei paties darbuotojo

veiksmai užtikrinant, kad konfidenciali informacija būtų naudojama tik darbo funkcijoms atlikti, nebūtų atskleista teisės su ja susipažinti neturintiems asmenims, nebūtų naudojama asmeniniams arba trečiųjų šalių interesams tenkinti, išskyrus teisės aktų nustatytus atvejus, kai darbuotojas turi teisę nesilaikyti išvardytų įsipareigojimų;

5.7. **Mobilieji įrenginiai** – tai specifinė turto kategorija, į kurią įeina tinklų ir informacinių sistemų įranga ir duomenų laikmenos, kurios gali būti lengvai perkeliamos ar naudojamos už organizacijos ribų (mobilieji telefonai, planšetės, nešiojamieji kompiuteriai ir pan.). Šis turtas dažnai naudojamas nuotoliniam darbui, mobiliajai prieigai prie organizacijos tinklų ir informacinių sistemų ar laikinosioms darbo vietoms;

5.8. **Serveris** – valstybinės archyvų sistemos įstaigos valdoma ar nuomojama fizinės ir (ar) virtualios techninės ir programinės įrangos visuma, apimanti tinklų ir informacinę sistemą ir ją sudarančią programinę įrangą bei duomenis;

5.9. **Tinklų ir informacinė sistema** (toliau – TIS) – elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais;

5.10. **Tinklų ir informacinių sistemų administratorius** (toliau – TIS administratorius) – valstybinės archyvų sistemos įstaigos darbuotojas, padalinys arba, jei atitinkama paslauga yra perkama, trečioji šalis (paslaugos teikėjas), atliekantis TIS priežiūrą, atsakingas už naujų tinklų ir informacinių sistemų paskyrų sukūrimą, sustabdymą ar panaikinimą, taip pat prieigų prie valstybinės archyvų sistemos įstaigų sistemos tinklų ir informacinių sistemų suteikimą, keitimą, sustabdymą ar panaikinimą pagal Prieigos užsakovo pateiktą prašymą ir tinklų bei informacinių sistemų savininko nurodymą. Jei paslauga perkama iš išorės, šias funkcijas pagal paslaugų teikimo sutartį atlieka paslaugos teikėjas, laikydamasis Tiekimo grandinės saugumo valdymo tvarkos aprašo reikalavimų;

5.11. **Tinklų ir informacinių sistemų savininkas** (toliau – TIS savininkas) valstybinės archyvų sistemos įstaigos darbuotojas, kuriam priskiriama atsakomybė už konkrečią tinklų ir informacinę sistemą visą jos gyvavimo organizacijoje ciklą;

5.12. **Turtas** – valstybinės archyvų sistemos įstaigos valdoma tinklų ir informacinė sistema, įskaitant techninę ir programinę įrangą bei duomenis. Prie turto priskiriamos ir tinklų ir informacinių sistemų dalys (kompiuterio pelės, klaviatūros);

5.13. **Turto registras** – šio Aprašo pagrindu parengtas ir nuolat atnaujinamas valstybinės archyvų sistemos įstaigos valdomo turto inventoriaus sąrašas, kurį sudaro valdomų tinklų ir informacinių sistemų sąrašas, valdomų serverių (tarnybinių ir darbo stočių) sąrašas, valdomos tinklo įrangos sąrašas, kitos valdomos techninės ar programinės įrangos sąrašai bei valdomų duomenų sąrašas;

5.14. **Turto naudotojas** – darbuotojas, turintis teisę naudotis valstybinės archyvų sistemos įstaigos turtu darbinėms funkcijoms atlikti. Turto naudotojais laikomi ir rangovai ar kiti įgalioti asmenys, turintys prieigą prie valstybinės archyvų sistemos įstaigos turto pagal savo pareigas, vykdomas funkcijas arba teikiamas paslaugas;

5.15. **Turto savininkas** – valstybinės archyvų sistemos įstaigos darbuotojas, kuriam priskirta atsakomybė už konkretų turtą visą jo gyvavimo organizacijoje ciklą;

5.16. **Trečioji šalis** – fizinis arba juridinis asmuo, turintis sutartinius ar kitus santykius su valstybinės archyvų sistemos įstaiga;

5.17. **Viešoji informacija** – visa valstybinės archyvų sistemos įstaigos interneto svetainėse, pranešimuose žiniasklaidai ir kitaip viešai platinama ar skelbiama informacija. Viešoji informacija tvarkoma ir skelbiama viešai teisės aktų nustatyta tvarka.

II SKYRIUS
ORGANIZACINĖS NUOSTATOS

6. Valstybinės archyvų sistemos įstaigos vadovas paskiria už turto valdymą atsakingus darbuotojus ir jiems priskiria šias funkcijas bei suteikia šiuos įgaliojimus.

7. Kibernetinio saugumo vadovo funkcijos ir įgaliojimai, susiję su turto valdymu:

7.1. rengia, nustatytu dažnumu peržiūri ir teikia tvirtinti šį Aprašą;

7.2. rengia ir teikia Lietuvos vyriausiajam archyvarui tvirtinti Leistinos programinės įrangos sąrašą;

7.3. kontroliuoja, kad turtas būtų valdomas vadovaujantis šio Aprašo nuostatomis;

7.4. kartu su TIS savininkais atlieka Turto registre numatytų valdomų TIS reikšmingumo vertinimą;

7.5. kartu su duomenų savininkais atlieka Turto registre numatytų valdomų duomenų svarbos vertinimą konfidencialumo, vientisumo ir prieinamumo atžvilgiu;

7.6. užtikrina, kad turto apsaugos priemonės atitiktų valstybinės archyvų sistemos įstaigos Tinklų ir informacinių sistemų kibernetinio saugumo politiką ir jos įgyvendinimą reglamentuojančių vidaus teisės aktų reikalavimus, taip pat TIS reikšmingumą ir duomenų svarbą;

7.7. vertina turto valdymo saugumo rizikas ir teikia rekomendacijas TIS ir (ar) Turto Duomenų savininkams dėl rizikų mažinimo;

7.8. identifikuoja ir stebi galimas grėsmes, susijusias su turto naudojimu, saugojimu ir šalinimu;

7.9. nustato turto naudojimo saugumo standartus ir užtikrina jų laikymąsi;

7.10. užtikrina, kad visi su turto saugumu susiję dokumentai ir informacija, ypač konfidenciali, būtų tinkamai tvarkoma ir saugoma pagal organizacijos reikalavimus;

7.11. kontroliuoja, kad už turto valdymą atsakingi darbuotojai visus reikiamus veiksmus atliktų šiame Apraše numatytu būdu;

7.12. užtikrina, kad trečiosios šalys, prieš jiems suteikiant prieigas prie TIS ir turto, parengtų ir šio Aprašo nustatyta tvarka pateiktų konfidencialumo laikymosi pasižadėjimus;

7.13. konsultuoja darbuotojus ir trečiąsias šalis dėl valstybinės archyvų sistemos įstaigos konfidencialios informacijos atskleidimo.

8. Turto savininko funkcijos ir įgaliojimai, susiję su turto ir konfidencialios informacijos valdymu:

8.1. atsako už turto naudojimą, priežiūrą ir apsaugą;

8.2. kontroliuoja turto perdavimo ir grąžinimo procesą;

8.3. koordinuoja turto gyvavimo ciklą, įskaitant jo įsigijimą, naudojimą, atnaujinimą ir utilizavimą;

8.4. atsako už valdomo turto įrašymą į įstaigos Turto registrą ir įrašų atnaujinimą, įskaitant valdomų serverių, operacinių sistemų (toliau – OS) ir tinklo įrangos sąrašų parengimą ir jų atnaujinimą pagal šio Aprašo 5–7 prieduose pateiktą Valdomų serverių sąrašo formą, Valdomų operacinių sistemų sąrašo formą ir Valdomos tinklo įrangos sąrašo formą;

8.5. užtikrina turto inventorizavimą ir duomenų aktualumą.

9. TIS savininko funkcijos ir įgaliojimai, susiję su Turto ir konfidencialios informacijos valdymu:

9.1. atlieka Turto registre numatytų valdomų TIS reikšmingumo vertinimą;

9.2. atsako už priskirto TIS valdymą;

9.3. atsako už valdomų TIS įrašymą į įstaigos Turto registrą ir įrašų atnaujinimą, t. y., valdomų TIS sąrašo parengimą ir atnaujinimą pagal šio Aprašo 4 priede pateiktą Valdomų Tinklų ir informacinių sistemų sąrašo formą;

9.4. atsako už valdomo TIS turto (pvz. laikmenų) sunaikinimą.

10. Duomenų savininko funkcijos ir įgaliojimai, susiję su turto valdymu:

10.1. atlieka Turto registre numatytų valdomų duomenų svarbos vertinimą konfidencialumo, vientisumo ir prieinamumo atžvilgiu;

10.2. prižiūri prieigos prie TIS kontrolę, užtikrindamas, kad prieiga būtų suteikta tik įgaliotiems asmenims ir pagal principą „būtina žinoti“;

10.3. atsako už valdomo turto įrašymą į įstaigos Turto registrą ir įrašų atnaujinimą, t. y., valdomų duomenų sąrašo parengimą ir atnaujinimą pagal šio Aprašo 8 priede pateiktą Valdomų duomenų sąrašo formą.

11. TIS administratoriaus funkcijos ir įgaliojimai, susiję su turto valdymu:

11.1. užtikrina, kad turtas būtų techniškai tvarkingas ir tinkamai funkcionuotų;

11.2. vykdo naujos TIS įrangos paruošimą ir konfigūravimą, įskaitant OS diegimą ir saugumo vertinimus bei OS, programinės įrangos atnaujinimus ir pataisų diegimus pagal TIS įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų atskleidimą, pataisų ir pokyčių valdymo tvarką;

11.3. koordinuoja turto naudojimo apribojimus pagal valstybinės archyvų sistemos įstaigos nustatytas saugumo taisykles ir kibernetinio saugumo vadovo rekomendacijas;

11.4. administruoja naudotojų prieigas;

11.5. dalyvauja turto inventorizacijoje.

III SKYRIUS
TURTO VALDYMAS

12. Turto valdymas apima turto identifikavimą, apskaitą, naudojimą, priežiūrą, saugojimą, perdavimą ir grąžinimą.

13. Turto valdymo proceso metu:

13.1. užtikrinama, kad visas turtas, už kurį atsako valstybinės archyvų sistemos įstaigos padaliniai, būtų tiksliai užregistruotas ir tvarkomas įstaigos Turto registre;

13.2. bet kokio kito specifinio Turto inventoriaus sąrašo tvarkymas turi būti visiškai suderintas su įstaigos Turto registru;

13.3. užtikrinamas turto perdavimo ir grąžinimo atsekamumas;

13.4. atliekami reguliarūs turto patikrinimai, siekiant užtikrinti, kad registruotas turtas atitinka realią situaciją ir nėra naudojamas Turto registre neregistruotas turtas;

13.5. TIS techninės įrangos gedimai turi būti registruojami;

13.6. TIS įrangos priežiūrą ir gedimų šalinimą turi atlikti kvalifikuoti specialistai;

13.7. renkama ir tvarkoma informacija apie turtą, reikalinga informacijos ir kibernetinio saugumo valdymui.

14. Prieš TIS įdiegimą ir naudojimą įstaigos Turto registre turi būti užregistruojama TIS ir visas su TIS susijęs turtas.

15. Turtą apskaitant, informacija apie jį turi būti surenkama ir suvedama į Turto registrą, kurį sudaro valdomų TIS, OS ir serverių ir tinklo įrangos bei kitos valdomos techninės ar programinės įrangos sąrašai.

16. Turto savininkai turi parengti ir ne rečiau kaip kartą per metus atnaujinti valstybinės archyvų sistemos įstaigos valdomo turto, įskaitant serverius, OS ir tinklo įrangą, sąrašus pagal šio Aprašo 5–7 prieduose pateiktą Valdomų serverių sąrašo formą, Valdomų operacinių sistemų sąrašo formą ir Valdomos tinklo įrangos sąrašo formą. Pasikeitus turto sudėčiai, įstaigos valdomo turto sąrašas turi būti atnaujinamas.

17. TIS savininkai turi parengti ir ne rečiau kaip kartą per metus atnaujinti įstaigos valdomų TIS sąrašą pagal šio Aprašo 4 priede pateiktą Valdomų tinklų ir informacinių sistemų sąrašo formą. Pasikeitus turto sudėčiai, įstaigos valdomo turto sąrašas turi būti atnaujintas.

18. Duomenų savininkai turi parengti ir ne rečiau kaip kartą per metus atnaujinti įstaigos valdomų duomenų sąrašą pagal šio Aprašo 8 priede pateiktą Valdomų duomenų sąrašo formą. Pasikeitus turto sudėčiai, įstaigos valdomo turto sąrašas turi būti atnaujintas.

19. Turto savininkai yra materialiai atsakingi už jiems priskirtą turtą. Turtą perdavus turto naudotojams, pastarieji tampa materialiai atsakingi už jiems perduotą turtą.

20. Turto perkėlimas už valstybinės archyvų sistemos įstaigų ribų galimas tik darbinėms funkcijoms atlikti. Darbuotojas turi užtikrinti nešiojamosios įrangos fizinę apsaugą, o perkeliant stacionarų turtą reikalingas turto savininko sutikimas.

21. Darbuotojas, nutraukęs darbo santykius su valstybinės archyvų sistemos įstaiga, privalo grąžinti jam patikėtą įstaigos turtą. Trečiosios šalies atveju darbuotojas, atsakingas už sutarties vykdymą, yra atsakingas ir už išduoto turto grąžinimą pasibaigus sutarties su trečiąja šalimi terminui ar iki galo suteikus paslaugą.

21.1. Grąžinus turtą, nedelsiant panaikinamos visos prieigos prie TIS;

21.2. Nurašant įrangą ar laikmenas, visa jose esanti informacija privalo būti ištrinta. Konfidenciali informacija turi būti pašalinta neatkuriamai, saugiu būdu, atliekant bent kelių ciklų perrašymą, arba fizinės laikmenos turi būti sunaikintos.

22. Programinės įrangos, kuri nėra įtraukta į Leistinos programinės įrangos sąrašą, diegimo reikalavimai:

22.1. darbuotojams draudžiama savarankiškai diegti programinę įrangą, kuri nėra įtraukta į Leistinos programinės įrangos sąrašą;

22.2. Iškilus poreikiui įdiegti darbo funkcijoms atlikti reikalingą programinę įrangą,

neįtrauktą į Leistinos programinės įrangos sąrašą, darbuotojas per IT pagalbos portalą arba el. paštu pateikia motyvuotą prašymą TIS administratoriui, nurodydamas programinės įrangos paskirtį, planuojamą naudojimą, duomenų pobūdį ir skubumo pagrindimą. Šis prašymas turi būti suderintas su tiesioginiu vadovu, įvertinant poreikio pagrįstumą ir patvirtinant, kad nėra tinkamos alternatyvos iš patvirtinto Leistinos programinės įrangos sąrašo;

22.3. TIS administratorius įvertina programinės įrangos techninį suderinamumą, licencijavimo sąlygas ir galimą poveikį informacinei infrastruktūrai;

22.3. Sprendimą dėl leidimo diegti programinę įrangą, kuri nėra įrašyta į Leistinos programinės įrangos sąrašą, priima TIS administratorius kartu su kibernetinio saugumo vadovu. Priėmus teigiamą sprendimą programinė įranga diegiama centralizuotai, registruojama įstaigos Turto registre ir ja leidžiama naudotis nustatytomis sąlygomis, o neigiamo sprendimo atveju darbuotojas informuojamas apie atsisakymo leisti diegti prašomą programinę įrangą motyvus;

22.4. Jei programinės įrangos poreikis yra skubus ir susijęs su veiklos tęstinumo užtikrinimu ar incidento valdymu, TIS administratorius gali suteikti laikiną leidimą ją įdiegti, nedelsiant informuodamas kibernetinio saugumo vadovą ir per nustatytą terminą atlikęs pilną rizikos vertinimą. Laikinas leidimas galioja, iki bus priimtas galutinis sprendimas;

22.5. Patvirtinta programinė įranga įtraukiama į Leistinos programinės įrangos sąrašą ne vėliau kaip artimiausios ketvirtinės peržiūros metu arba, esant poreikiui, sąrašas papildomas nedelsiant. Visi veiksmai – prašymas, vertinimas, sprendimas ir įtraukimas į sąrašą – fiksuojami IT pagalbos portale.

23. Keičiamųjų duomenų laikmenų naudojimo reikalavimai:

23.1. Keičiamosios duomenų laikmenos (USB atmintinės, išoriniai diskai, SD kortelės ir pan.) turi būti apskaitomos įstaigos Turto registre. Draudžiama naudoti privačias keičiamąsias laikmenas valstybinės archyvų sistemos įstaigos duomenims saugoti ar perduoti;

23.2. Keičiamosios laikmenos, kuriose saugomi konfidencialūs duomenys, prieš jas išnešant iš valstybinės archyvų sistemos įstaigos patalpų turi būti šifruojamos;

23.3. Nereikalingos ar nurašomos keičiamosios laikmenos turi būti sunaikinamos arba jose esantys duomenys turi būti neatkuriamai ištrinti pagal šio Aprašo 21.2 papunkčio reikalavimus, prieš laikmeną perduodant, utilizuojant ar sunaikinant;

23.4. Rastos ar neidentifikuotos laikmenos negali būti prijungiamos prie valstybinės archyvų sistemos įstaigų įrangos – apie jas nedelsiant informuojamas kibernetinio saugumo vadovas;

23.5. Keičiamųjų laikmenų naudojimas gali būti apribotas techninėmis priemonėmis pagal šio Aprašo 24.7 papunkčio reikalavimus.

24. Valstybinės archyvų sistemos įstaigos atsakingi darbuotojai turi įgyvendinti šiuos reikalavimus, keliamus mobiliųjų įrenginių saugumui:

24.1. visi mobilieji įrenginiai, valstybinės archyvų sistemos įstaigoje naudojami duomenims pasiekti ar saugoti, turi būti apskaitomi vadovaujantis šio Aprašo reikalavimais;

24.2. mobilieji įrenginiai, turintys prieigą prie TIS, ir juose įdiegta programinė įranga turi būti valdomi centralizuotai;

24.3. mobiliuosiuose įrenginiuose privalo būti įdiegtos priemonės, leisiančios nuotoliniu būdu neatkuriamai ištrinti mobiliuosiuose įrenginiuose esančius duomenis;

24.4. mobilieji įrenginiai, kuriais naršoma internete, turi būti apsaugoti nuo judriųjų programų (angl. *mobile code*) keliamų grėsmių;

24.5. išorinės laikmenos su konfidencialiais duomenimis, prieš jas išnešant iš valstybinės archyvų sistemos įstaigos, turi būti šifruojamos;

24.6. perkeliant duomenis už valstybinės archyvų sistemos įstaigos ribų, turi būti taikomi tinkami šifravimo ir autentifikacijos mechanizmai;

24.7. valstybinės archyvų sistemos įstaigose turi būti naudojamos techninės priemonės, kurios apribotų neleistinų, į įstaigos Turto registrą neįrašytų įrenginių prijungimą prie TIS ir neleistinos techninės įrangos naudojimą, o apie bandymus neteisėtai prisijungti informuotų kibernetinio saugumo vadovą.

25. Mobiliųjų įrenginių naudotojų atsakomybės:

25.1. įstaigos išduotus mobiliuosius įrenginius darbuotojai gali naudoti tik darbo funkcijoms vykdyti;

25.2. išduotuose mobiliuosiuose įrenginiuose draudžiama diegti trečiųjų šalių ar bet kokią kitą programinę įrangą, kuri nėra būtina darbo funkcijoms atlikti arba nėra suderinta su kibernetinio saugumo vadovu;

25.3. draudžiama dirbti viešuose ar nesaugiuose tinkluose, nebent kompiuteryje yra įdiegta ir veikianti „Always On VPN" technologija;

25.4. praradus mobilųjį įrenginį, laikmeną ar kitą perkeliamą turtą privaloma kaip įmanoma greičiau, bet ne vėliau kaip kitą darbo dieną, informuoti kibernetinio saugumo vadovą ir už šio turto apskaitą atsakingą darbuotoją;

25.5. visus mobiliuosius įrenginius apsaugoti slaptažodžiu, PIN kodu ar biometrinėmis priemonėmis (pvz., piršto atspaudu, veido atpažinimu);

25.6. visuose įrenginiuose, naudojančiuose ar saugančiuose valstybinės archyvų sistemos įstaigos duomenis, būtina įjungti duomenų šifravimo funkcionalumus.

IV SKYRIUS
TURTO IR DUOMENŲ VERTINIMAS IR KLASIFIKAVIMAS

26. Kibernetinio saugumo vadovas kartu su TIS savininku, vadovaudamiesi Tinklų ir informacinių sistemų veiklos tęstinumo valdymo tvarkos aprašo nustatyta tvarka pateikta poveikio veiklai vertinimo metodika, turi atlikti valdomos TIS reikšmingumo vertinimą, nustatydami, ar TIS turi poveikį valstybinės archyvų sistemos įstaigos kritiniam procesui (paslaugai), ir tuo pagrindu TIS priskirdami prie reikšmingų ir nereikšmingų TIS grupės. Kibernetinio saugumo vadovas TIS reikšmingumo vertinimo rezultatus turi įrašyti į Valdomų tinklų ir informacinių sistemų sąrašą pagal šio Aprašo 4 priede pateiktą Valdomų tinklų ir informacinių sistemų sąrašo formą.

27. Kibernetinio saugumo vadovas, vadovaudamasis Kibernetinio saugumo įstatymo 13 straipsnio 3 dalies 7 punkto nuostatomis, visas reikšmingas TIS turi įrašyti į Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos administruojamą Kibernetinio saugumo informacinę sistemą.

28. Kibernetinio saugumo vadovas kartu su duomenų savininkais turi atlikti Turto registre numatytų duomenų svarbos vertinimą konfidencialumo, vientisumo ir prieinamumo atžvilgiu. Atliekant vertinimą vadovaujamasi Valstybės informacinių išteklių svarbos vertinimo tvarkos aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2024 m. gegužės 15 d. nutarimu Nr. 349 „Dėl Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo įgyvendinimo". Kibernetinio saugumo vadovas atlikto vertinimo rezultatus turi įrašyti į Valdomų duomenų sąrašą pagal šio Aprašo 8 priede pateiktą Valdomų duomenų sąrašo formą.

29. Kibernetinio saugumo vadovas duomenų svarbos vertinimo pagrindu visus valstybinės archyvų sistemos įstaigos valdomus duomenis turi suskirstyti į dvi grupes: vieša informacija bei konfidenciali informacija. Būtina užtikrinti, kad taikomos kibernetinio saugumo priemonės būtų proporcingos duomenų svarbai.

V SKYRIUS
BAIGIAMOSIOS NUOSTATOS

30. Šis Aprašas turi būti peržiūrimas ir atnaujinamas bent kartą per metus arba atsiradus esminių pokyčių, galinčių turėti įtakos šiam Aprašui. Už šio Aprašo peržiūrėjimą ir atnaujinimą yra atsakingas kibernetinio saugumo vadovas. Šis Aprašas peržiūrimas pagal šio Aprašo 1 priede nustatytą apskaitos žurnalo formą.

_____

Turto valdymo tvarkos aprašo
1 priedas

(Apskaitos žurnalo forma)

TURTO VALDYMO TVARKOS PERŽIŪROS APSKAITOS ŽURNALAS

Dokumento versija	Veiklos data	Statusas	Atsakingas asmuo	Pagrindinės korekcijos	Patvirtinimo data ir Nr.

_____

Turto valdymo tvarkos aprašo
2 priedas

(Turto perdavimo ir gąžinimo akto forma)

TURTO PERDAVIMO IR GRĄŽINIMO AKTAS

20__m._____d

Turto naudotojas:

_____

(Pareigos, vardas, pavardė)

Turto savininkas / atsakingas už apskaitą asmuo:

_____

(Pareigos, vardas, pavardė)

Eil. Nr.	Turto pavadinimas	Apskaitos numeris	Serijos numeris	Perdavimo tikslas	Grąžinimo terminas

Turto perdavimo sąlygos:

☐ Turtas perduodamas darbinėms funkcijoms vykdyti organizacijos patalpose

☐ Turtas perduodamas naudoti už organizacijos ribų (nurodyti tikslą): _____

☐ Kita: _____

Naudotojas patvirtina, kad:

– susipažino su Turto valdymo tvarkos apraše nustatytais reikalavimais;

– įsipareigoja turtą naudoti tik darbinėms funkcijoms;

– įsipareigoja grąžinti turtą nustatytu terminu arba nutraukdamas darbo santykius.

Turto savininkas: _____ (parašas) Data: _____

Turto naudotojas: _____(parašas) Data: _____

Turto grąžinimas (pildoma grąžinant):

Grąžinimo data: _____

Turto būklė: ☐ Tinkama ☐ Pažeista (aprašyti): _____

Prieigos panaikintos: ☐ Taip ☐ Ne (nurodyti priežastį): _____

Priėmė: _____ (parašas)

_____

Turto valdymo tvarkos aprašo
3 priedas

(Konsfidencialumo pasižadėjimo forma)

KONFIDENCIALUMO LAIKYMOSI PASIŽADĖJIMAS

20__m._____d.

[Vieta]

1. Aš, _____ _____

,

(Pareigos, vardas ir pavardė, atstovaujamo juridinio asmens pavadinimas, jei taikoma)

pasirašydamas (-a) šį pasižadėjimą, įsipareigoju griežtai saugoti [Organizacijos pavadinimas] (toliau – [Organizacijos pavadinimo trumpinys]) konfidencialią informaciją vykdant su [Organizacijos pavadinimo trumpinys]) sudarytą sutartį Nr. _____ (toliau – Sutartis) ir (arba) teikiant paslaugas.

2. Pripažįstu, kad atlikdamas (-a) sutartyje ar kituose susitarimuose nurodytas funkcijas bei vykdydamas (-a) įsipareigojimus, galiu gauti ir gausiu konfidencialią informaciją, kuri yra išskirtinė [Organizacijos pavadinimo trumpinys] ar jai tokią informaciją suteikusių trečiųjų asmenų nuosavybė.

3. Konfidenciali informacija – [Organizacijos pavadinimo trumpinys] disponuojama nevieša, vertinga ir saugoma informacija, užfiksuota popierine ar elektronine forma ir [Organizacijos pavadinimo trumpinys] disponuojami viešai neskelbtini asmens duomenys, kurių atskleidimas gali sukelti neigiamą poveikį organizacijai ar tretiesiems asmenims, įskaitant fizinius asmenis.

4. **Pasižadu:**

4.1. neatskleisti tretiesiems asmenims duomenų, sudarančių [Organizacijos pavadinimo trumpinys] konfidencialią informaciją, nei sutarties galiojimo metu, nei jai pasibaigus, išskyrus atvejus, kai informaciją atskleisti reikalauja Lietuvos Respublikos įstatymai arba gavus išankstinį raštišką [Organizacijos pavadinimo trumpinys] sutikimą;

4.2. naudoti gautą konfidencialią informaciją išimtinai tik [Organizacijos pavadinimo trumpinys] interesais ir sutartyje numatytų funkcijų vykdymui;

4.3. saugoti gautą konfidencialią informaciją nuo neteisėto atskleidimo, praradimo, sunaikinimo ir imtis visų būtinų techninių bei organizacinių priemonių, kad tokia informacija nebūtų prieinama tretiesiems asmenims;

4.4. informuoti kitus atstovaujamos trečiosios šalies darbuotojus ar subrangovus (kai jiems tokia informacija privalo būti perduodama funkcijoms atlikti) apie jiems perduotos informacijos konfidencialumą ir užtikrinti, kad jie laikytųsi šio pasižadėjimo reikalavimų;

4.5. pasibaigus sutarčiai ar [Organizacijos pavadinimo trumpinys] pareikalavus, nedelsiant grąžinti visas konfidencialios informacijos laikmenas, dokumentus ir (arba) neatkuriamai sunaikinti jos kopijas savo informacinėse sistemose.

5. Patvirtinu, kad:

5.1. Man išaiškinta, kokia informacija laikoma konfidencialia, ir esu įspėtas (-a), kad tiek tyčiniais veiksmais, tiek dėl neatsargumo pažeidęs (-usi) bet kurį iš šiame pasižadėjime nurodytų įsipareigojimų, privalėsiu atlyginti [Organizacijos pavadinimo trumpinys] padarytus tiesioginius ir netiesioginius nuostolius.

5.2. Šiame pasižadėjime nurodytų įsipareigojimų pažeidimas bus laikomas esminiu sutarties pažeidimu, suteikiančiu teisę [Organizacijos pavadinimo trumpinys] vienašališkai ir nedelsiant nutraukti paslaugų teikimo ar bendradarbiavimo sutartį bei taikyti sutartines sankcijas.

_____ _____

(Atstovaujamos trečiosios šalies pavadinimas, pareigos, vardas, pavardė) (Parašas)

_____

Turto valdymo tvarkos aprašo
4 priedas

(Valdomų tinklų ir informacinių sistemų sąrašo forma)

VALDOMŲ TINKLŲ IR INFORMACINIŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	**TIS pavadinimas**	**TIS reikšmingumas**	**TIS savininkas**	**TIS administratorius**	**Palaikymo statusas**	**Palaikymo pabaigos data**	**TIS laikymo vieta**
	1	***2***	***3***	***4***	***5***	***6***	***7***

[Pildymo instrukcija.
[1] nurodomas TIS pavadinimas, kaip ji vadinama organizacijoje (pvz. finansų valdymo TIS) arba nurodomas gamintojo naudojamas pavadinimas (pvz. SharePoint, Teams, Google Drive ir pan.);
[2] TIS reikšmingumas nurodomas pagal organizacijos atsakingų asmenų atliktą poveikio veiklai vertinimą, TIS priskiriant prie šių grupių: (i) Reikšminga TIS; (ii) Nereikšminga TIS;
[3] nurodomos organizacijos darbuotojo, atsakingo už TIS priežiūrą ir palaikymą, ir (ar) atsakingo paslaugų tiekėjo, kuris prižiūri ir atsako už sutartinių įsipareigojimų vykdymo kontrolę, pareigos, vardas, pavardė;
[4] nurodomos organizacijos darbuotojo, kuriam suteikti įgaliojimai administruoti konkrečią TIS, sukurti, sustabdyti ar panaikinti TIS naudotojų paskyras ir (ar) suteikti, sustabdyti ar panaikinti TIS naudotojų prieigas prie TIS, pareigos, vardas, pavardė;
[5] nurodoma, ar TIS yra palaikoma jos gamintojo ir (ar) paslaugų tiekėjo;
[6] nurodoma, kada baigiasi gamintojo TIS palaikymas (angl. End of support);
[7] nurodoma aplinka, kurioje yra įdiegta TIS (pvz. fiziniai ir (ar) virtualūs serveriai ar debesijos infrastruktūra ir pan.)].

_____

Turto valdymo tvarkos aprašo
5 priedas

(Valdomų serverių sąrašo forma)

VALDOMŲ SERVERIŲ SĄRAŠAS

Eil. Nr.	Serverio tipas	Serverio pavadinimas	Turto savininkas	Apskaitos numeris	Serverio vieta	Tarnybinė stotis (angl. *Host*)	Serverio IP adresas	Tinklo pavadinimas	Serverio parametrai						Įsigijimo data	Turto valdymo pagrindas (sutartis)	Garantija	Palaikymas	OS
									Gamintojas	Modelis	Serijos numeris	CPU	HDD/ SSD	Kita					
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*	15	*16*	*17*	*18*	*19*

[Pildymo instrukcija.
[1] nurodoma, ar serveris yra fizinis – ar virtualus;
[2] nurodomas serverio pavadinimas;
[3] nurodomos organizacijos darbuotojo, atsakingo už serverio priežiūrą ir palaikymą, ir (ar) atsakingo už paslaugų tiekėjo, kuris prižiūri ir palaiko serverius, atsako už sutartinių įsipareigojimų vykdymo kontrolę, pareigos, vardas, pavardė;
[4] nurodomas inventorizacijos numeris apskaitos dokumentuose (jei tokia apskaita vykdoma);
[5] nurodomas patalpų, kuriose stovi serveris, pavadinimas ir adresas arba trečiųjų šalių paslaugų teikėjo pavadinimas ir duomenų centro adresas;
[6] nurodomas tarnybinės stoties vardas (pavadinimas);
[7] nurodomas serverio IP adresas;
[8] nurodomas serverio tinklo pavadinimas;
[9] nurodomas serverio gamintojo pavadinimas;
[10] nurodomas serverio modelio pavadinimas;
[11] nurodomas serverio serijos numeris;
[12] nurodomas serverio centrinio procesoriaus (angl. CPU) pavadinimas;
[13] nurodomas serverio kietojo disko tipas ir pavadinimas (angl. HDD ar SSD);
[14] esant poreikiui nurodomi papildomi serverio parametrai;
[15] nurodoma data, kada serveris buvo įsigytas;
[16] nurodoma įsigijimo ar nuomos sutartis;
[17] nurodoma, ar yra suteikta garantija serveriui ir kuriam laikui pvz.: Taip – 2 metams;
[18] nurodomas visuotinis gamintojo palaikymas (angl. End of support date);

[19] nurodoma įrenginio operacinė sistema (Windows, Linux ir t.t.)].

Turto valdymo tvarkos aprašo
6 priedas

(Valdomų operacinių sistemų sąrašo forma)

VALDOMŲ OPERACINIŲ SISTEMŲ SĄRAŠAS

Eil. Nr.	**OS pavadinimas**	**Versija**	**Gamintojas**	**Architektūra**	**Licencijos tipas**	**Licencijos galiojimas**	**Naudojimo sritis**	**Diegimo aplinka**	**Turto savininkas**	**TIS administratorius**	**Pastabos**
1	***2***	***3***	***4***	***5***	***6***	***7***	***8***	***9***	***10***	***11***

[Pildymo instrukcija.
[1] nurodomas tikslus serverio ar duomenų bazės operacinės sistemos pavadinimas (pvz.: Windows 11, Ubuntu 22.04);
[2] nurodoma konkreti operacinės sistemos versija arba leidimas (pvz.: 21H2, LTS, Enterprise);
[3] nurodomas operacinės sistemos kūrėjas (pvz.: Microsoft, Apple, Canonical);
[4] nurodoma, ar sistema yra 32-bit ar 64-bit (pvz.: x86, x64, ARM);
[5] nurodomas licencijos tipas (pvz.: komercinė, nemokama, atvirojo kodo);
[6] nurodomas licencijos galiojimo laikas;
[7] nurodoma, kokiam tikslui naudojama OS (pvz.: darbo stotims, serveriams, testavimui);
[8] nurodoma aplinka, kurioje įdiegta OS (pvz.: lokali, debesija, virtuali mašina);
[9] nurodomas padalinys ar asmuo, atsakingi už OS naudojimą ir sprendimų dėl jos poreikio įstaigoje priėmimą;
[10] nurodomas asmuo ar komanda, atsakingi už OS diegimą, konfigūravimą ir techninę priežiūrą (sistemos (arba serverio) administratorius);
[11] papildoma informacija (pvz., specifiniai reikalavimai ar apribojimai.].

Turto valdymo tvarkos aprašo
7 priedas

(Valdomų tinklo įrangos sąrašo forma)

VALDOMOS TINKLO ĮRANGOS SĄRAŠAS

Eil. Nr.	Įrenginio pavadinimas	Apskaitos numeris	Vieta	TIS administratorius	Įrangos parametrai				Įsigijimo data	Turto valdymo pagrindas (sutartis)	Garantija	Palaikymas	OS	Kita
					Gamintojas	Modelis	Serijos numeris	Kita						
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*	*12*	*13*	*14*

[Pildymo instrukcija.
[1] nurodomas įrenginio pavadinimas (pagal paskirtį) (pvz.: maršrutizatorius, komutatorius, ugniasienė ir pan.);
[2] nurodomas inventorizacijos numeris apskaitos dokumentuose;
[3] nurodomas patalpos, kuriame stovi įrenginys, pavadinimas arba trečiųjų šalių paslaugų teikėjo duomenų centras;
[4] nurodomas už tinklo įrenginio priežiūrą atsakingas asmuo;
[5] nurodomas įrenginio gamintojo pavadinimas;
[6] nurodomas įrenginio modelio pavadinimas;
[7] nurodomas įrenginio serijos numeris;
[8] esant poreikiui nurodoma papildoma svarbi informacija apie įrenginį;
[9] nurodoma įrenginio įsigijimo data;
[10] nurodoma įsigijimo ar nuomos sutartis;
[11] nurodoma, ar yra suteikta garantija įrenginiui ir kuriam laikui;
[12] nurodomas visuotinis gamintojo palaikymas (angl. End of support date);

[13] nurodoma įrenginio operacinė sistema (Windows, Linux ir t.t.);
[14] esant poreikiui nurodoma papildoma svarbi informacija.].

Turto valdymo tvarkos aprašo
8 priedas

(Valdomų duomenų sąrašo forma)

VALDOMŲ DUOMENŲ SĄRAŠAS

Eil. Nr.	Duomenų grupės pavadinimas	Duomenų aprašymas	Duomenų forma	Duomenų svarbos kategorija	Asmens duomenų kategorija	Duomenų savininkas	Duomenų tvarkymo tikslai	Duomenų tvarkymo teisinis pagrindas	Duomenų saugojimo vieta	Duomenų saugojimo terminas	Kita
	1	*2*	*3*	*4*	*5*	*6*	*7*	*8*	*9*	*10*	*11*

[Pildymo instrukcija.
[1] nurodomas duomenų grupės pavadinimas (pvz.: darbuotojų duomenys, finansinės apskaitos duomenys ir pan.);
[2] pateikiamas duomenų aprašymas (pvz., darbuotojų darbo bylos duomenys);
[3] nurodoma duomenų forma: elektroniniai ar popieriniai duomenys;
[4] nurodoma duomenų svarbos kategorija: labai svarbūs, svarbūs, vidutinės svarbos ar mažos svarbos duomenys;
[5] nurodoma asmens duomenų kategorija: paprasti asmens duomenys, specialiosios kategorijos asmens duomenys, ypatingi asmens duomenys. Jei duomenys nesudaro asmens duomenų, nurodoma „ne asmens duomenys";
[6] nurodomos darbuotojo, atsakingo už duomenų valdymą ir (ar) tvarkymą, pareigos, vardas ir pavardė;
[7] nurodomi duomenų tvarkymo tikslai (pvz., personalo valdymas);
[8] nurodomas duomenų tvarkymo teisinis pagrindas (pvz., Lietuvos Respublikos darbo kodeksas);
[9] nurodoma duomenų saugojimo vieta (pvz.: personalo valdymo informacinė sistema, file serveris arba saugykla);
[10] nurodomas įstatymais reglamentuotas duomenų saugojimo terminas. Jei duomenų saugojimo terminas įstatymuose nėra numatytas, duomenų savininkas nustato maksimalų duomenų saugojimo terminą;

[11] esant poreikiui nurodoma papildoma svarbi informacija.].

DETALŪS METADUOMENYS	
Dokumento sudarytojas (-ai)	Lietuvos vyriausiojo archyvaro tarnyba 188697087, Mindaugo g. 8, Vilnius
Dokumento pavadinimas (antraštė)	ĮSAKYMAS DĖL LIETUVOS VYRIAUSIOJO ARCHYVARO TARNYBOS IR VALSTYBĖS ARCHYVŲ KIBERNETINIO SAUGUMO VALDYMO DOKUMENTŲ PATVIRTINIMO
Dokumento registracijos data ir numeris	2026-04-17 Nr. VE1-7
Dokumento gavimo data ir dokumento gavimo registracijos numeris	–
Dokumento specifikacijos identifikavimo žymuo	ADOC-V1.0
Parašo paskirtis	Suderinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Darius Baronas, Skyriaus vedėjas, Duomenų ir skaitmeninio išsaugojimo sprendimų skyrius
Sertifikatas išduotas	DARIUS BARONAS LT
Parašo sukūrimo data ir laikas	2026-04-16 13:30:33 (GMT+03:00)
Parašo formatas	XAdES-EPES
Laiko žymoje nurodytas laikas	–
Informacija apie sertifikavimo paslaugų teikėją	SK ID Solutions EID-Q 2021E, SK ID Solutions AS EE
Sertifikato galiojimo laikas	2024-11-14 16:49:40 – 2029-11-14 23:59:59
Parašo paskirtis	Suderinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Gintaras Dručkus, Direktorius, Administracija
Sertifikatas išduotas	GINTARAS DRUČKUS LT
Parašo sukūrimo data ir laikas	2026-04-16 13:52:46 (GMT+03:00)
Parašo formatas	XAdES-EPES
Laiko žymoje nurodytas laikas	–
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2024-08-09 11:15:09 – 2029-08-08 23:59:59
Parašo paskirtis	Pasirašymas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Inga Zakšauskienė, Lietuvos vyriausioji archyvarė
Sertifikatas išduotas	INGA ZAKŠAUSKIENĖ LT
Parašo sukūrimo data ir laikas	2026-04-17 14:28:02 (GMT+03:00)
Parašo formatas	XAdES-X-L
Laiko žymoje nurodytas laikas	2026-04-17 14:28:15 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2022-12-23 11:17:12 – 2027-12-22 23:59:59
Parašo paskirtis	Susipažinimas
Parašą sukūrusio asmens vardas, pavardė ir pareigos	Vida Jakimavičienė, Vyriausioji specialistė, Veiklos administravimo ir finansų skyrius
Sertifikatas išduotas	VIDA JAKIMAVIČIENĖ LT
Parašo sukūrimo data ir laikas	2026-06-09 19:41:39 (GMT+03:00)
Parašo formatas	XAdES-X-L
Laiko žymoje nurodytas laikas	2026-06-09 19:41:55 (GMT+03:00)
Informacija apie sertifikavimo paslaugų teikėją	EID-SK 2016, AS Sertifitseerimiskeskus EE
Sertifikato galiojimo laikas	2022-05-09 17:44:08 – 2027-05-08 23:59:59
Informacija apie būdus, naudotus metaduomenų vientisumui užtikrinti	"Registravimas" paskirties metaduomenų vientisumas užtikrintas naudojant "RCSC IssuingCA-2, VI Registru Centras - i.k. 124110246 LT" išduotą sertifikatą "DBSIS, Informatikos ir ryšių departamentas prie Lietuvos Respublikos vidaus reikalų ministerijos, į.k.188774822 LT", sertifikatas galioja nuo 2025-05-16 11:31:08 iki 2028-05-15 11:31:08
Pagrindinio dokumento priedų skaičius	14
Pagrindinio dokumento pridedamų dokumentų skaičius	–

DETALŪS METADUOMENYS	
Pridedamo dokumento sudarytojas (-ai)	–
Pridedamo dokumento pavadinimas (antraštė)	–
Pridedamo dokumento registracijos data ir numeris	–
Programinės įrangos, kuria naudojantis sudarytas elektroninis dokumentas, pavadinimas	DBSIS, versija 3.5.90.4
Informacija apie elektroninio dokumento ir elektroninio (-ių) parašo (-ų) tikrinimą (tikrinimo data)	Atitinka specifikacijos keliamus reikalavimus. Visi dokumente esantys elektroniniai parašai galioja (2026-08-24 14:06:40)
Paieškos nuoroda	–
Papildomi metaduomenys	Nuorašą suformavo 2026-08-24 14:06:41 DBSIS