LIETUVOS RESPUBLIKOS KRAŠTO APSAUGOS MINISTRAS

ĮSAKYMAS DĖL SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO NUOSTATŲ PATVIRTINIMO

2018 m. vasario 7 d. Nr. V-135
Vilnius

Vadovaudamasis Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 5 straipsnio 4 dalies 3 punktu ir 6 straipsnio 4 dalies 4 punktu,

t v i r t i n u Saugaus valstybinio duomenų perdavimo tinklo nuostatus.

Krašto apsaugos ministras Raimundas Karoblis

PATVIRTINTA
Lietuvos Respublikos krašto apsaugos ministro
2018 m. vasario 7 d. įsakymu
Nr. V-135

SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO NUOSTATAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Saugaus valstybinio duomenų perdavimo tinklo nuostatai (toliau – Nuostatai) reglamentuoja Saugaus valstybinio duomenų perdavimo tinklo (toliau – SVDPT) tikslus, uždavinius, funkcijas, organizacinę ir funkcinę struktūrą, reikalavimus duomenų saugai, tinklo finansavimo šaltinius, Saugaus valstybinio duomenų perdavimo tinklo paslaugų teikimo tvarką ir atlyginimo už tinklu teikiamas paslaugas dydžių nustatymo tvarką.

2. Nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos elektroninių ryšių įstatyme ir kituose su Nuostatais susijusiuose Lietuvos Respublikos teisės aktuose vartojamas sąvokas.

3. SVDPT tikslas – pateikti nuo viešųjų elektroninių ryšių tinklų (interneto) atskirtą ir apsaugotą bei viešai neteikiamą elektroninių ryšių tinklą visoms Lietuvos Respublikos valstybės ir savivaldybių institucijoms, įstaigoms ir įmonėms (toliau – Lietuvos Respublikos institucijos), kuris leistų saugiai teikti duomenis, bendradarbiauti su Europos Sąjungos institucijomis, užtikrinant duomenų mainų dalyvių tapatybės nustatymą, perduodamų duomenų konfidencialumą, vientisumą ir prieinamumą.

4. SVDPT uždaviniai:

4.1. sudaryti sąlygas Lietuvos Respublikos institucijoms saugiai ir efektyviai keistis informacija su Europos Sąjungos institucijomis ir Europos Sąjungos valstybių narių administracijomis;

4.2. sudaryti sąlygas Lietuvos Respublikos institucijoms saugiai ir efektyviai keistis informacija tarpusavyje ir tarp institucijų struktūrinių padalinių;

4.3. sudaryti sąlygas sumažinti Lietuvos Respublikos institucijų išlaidas duomenų saugos priemonėms, programinei įrangai, duomenų perdavimo ir telefono ryšio paslaugoms įsigyti;

4.4. sudaryti sąlygas Lietuvos Respublikos fiziniams ir juridiniams asmenims naudotis elektroninės valdžios (toliau – e. valdžia) paslaugomis, užtikrinant Lietuvos Respublikos fizinių ir juridinių asmenų saugų bendravimą su Europos Sąjungos ir valstybių narių administracijomis.

4.5. užtikrinti registrų ir valstybės informacinių sistemų duomenų saugų teikimą.

II SKYRIUS
SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO ORGANIZACINĖ STRUKTŪRA

5. SVDPT valdytojas – Lietuvos Respublikos krašto apsaugos ministerija.

6. SVDPT tvarkytojas – Lietuvos Respublikos Krašto apsaugos ministro įgaliota Valstybės įmonė „Infostruktūra“ (toliau – tvarkytojas).

7. SVDPT valdytojas atlieka šias funkcijas:

7.1. koordinuoja SVDPT tvarkytojo darbą, nustatyta tvarka atlieka jo priežiūrą;

7.2. atlieka saugos reikalavimų laikymosi priežiūrą;

7.3. nagrinėja SVDPT tvarkytojo pasiūlymus dėl SVDPT veiklos tobulinimo ir priima dėl jų sprendimus;

7.4. užtikrina, kad SVDPT būtų tvarkomas vadovaujantis SVDPT nuostatais ir kitais teisės aktais.

8. SVDPT tvarkytojas atlieka šias funkcijas:

8.1. stebi, valdo ir prižiūri visą SVDPT komunikacinę įrangą ir ryšio linijas;

8.2. stebi, valdo ir prižiūri duomenų saugos įrangą ir priemones;

8.3. rengia Lietuvos Respublikos institucijų prijungimo prie SVDPT ar institucijų struktūrinių padalinių sujungimo techninius projektus;

8.4. įrengia ir valdo ryšio linijas ir aparatūrą, kurios reikia prijungimui prie SVDPT ir perduodamų duomenų saugumui užtikrinti;

8.5. užtikrina SVDPT funkcijų, nurodytų Nuostatų III skyriuje, vykdymą;

8.6. dalyvauja Europos viešojo administravimo institucijų, įskaitant vietos ir regionų viešojo administravimo institucijas ir Bendrijos institucijas, sąveikumo sprendimų programoje, kuria užtikrinami bendrieji sąveikumą skatinantys sprendimai (toliau – Sąveikumo programa) veikloje, atstovaudamas Lietuvos Respublikos nacionaliniam valstybės institucijų tinklo domenui ir yra Europos Sąjungos administracijų telematinio elektroninių ryšių tinklo TESTA (angl. *Trans-European Services for Telematics between Administrations*) (toliau – TESTA) nacionalinis techninis atstovas (angl. TESTA *National Technical Contact*);

8.7. dalyvauja TESTA ekspertų grupių veikloje atstovaudamas Lietuvos Respublikos nacionaliniam TESTA domenui;

8.8. atlieka Sąveikumo programos paslaugų priežiūrą Lietuvos Respublikoje;

8.9. administruoja interneto adresų sritis, naudojamas bendroms Lietuvos Respublikos institucijų reikmėms.

9. SVDPT tvarkytojas atlieka šias funkcijas:

9.1. nepertraukiamai teikia SVDPT paslaugas 24 valandas per parą ir 7 dienas per savaitę;

9.2. atsako už SVDPT paslaugų teikimo sutartimi tarp SVDPT tvarkytojo ir Lietuvos Respublikos institucijos nustatytą teikiamų paslaugų kokybę;

9.3. užtikrina SVDPT perduodamų duomenų saugą pagal sąlygas, nustatytas SVDPT paslaugų teikimo sutartimi tarp SVDPT tvarkytojo ir Lietuvos Respublikos institucijos;

9.4. užtikrina TESTA ir kitų Sąveikumo programos tinklų paslaugų teikimo kokybę ir saugumą pagal sąlygas, nustatytas sutartimi tarp Europos Bendrijos Sąveikumo programos komisijos ir Lietuvos Respublikos Vyriausybės įgaliotos institucijos.

10. SVDPT tvarkytojas turi teisę:

10.1. pasitelkti trečiuosius asmenis visiems savo sutartiniams įsipareigojimams vykdyti;

10.2. nustatyti atlyginimo už SVDPT teikiamas paslaugas dydžius, nedidinant Nuostatų 26 punkte nurodytų SVDPT valdytojo patvirtintų atlyginimo už naudojimąsi SVDPT dydžių;

10.3. reikalauti sumokėti už teikiamas paslaugas;

10.4. sustabdyti paslaugų teikimą, jeigu Lietuvos Respublikos institucija laiku neatsiskaitė už teikiamas paslaugas arba iš esmės pažeidė SVDPT paslaugų teikimo taisyklių nuostatas ar Lietuvos Respublikos institucijos veiksmai gali sukelti neigiamų padarinių SVDPT ir padaryti žalos jam ar kitoms prie jo prijungtoms Lietuvos Respublikos institucijoms.

11. SVDPT tvarkytojas, vykdydamas jam pavestas funkcijas, prekių ir paslaugų pirkimus atlieka vadovaudamasis Lietuvos Respublikos viešųjų pirkimų įstatymu.

III SKYRIUS
SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO FUNKCINĖ STRUKTŪRA

12. SVDPT, įgyvendindamas 4.1 uždavinį, atlieka šias funkcijas:

12.1. sudaro sąlygas teikti TESTA ir kitų Sąveikumo programos tinklų paslaugas Lietuvos Respublikos institucijoms ir teikia saugaus duomenų perdavimo paslaugas Lietuvos Respublikoje;

12.2. sudaro sąlygas Lietuvos Respublikos valstybės institucijų viešųjų raktų katalogų sertifikavimo įstaigai keistis duomenimis su Sąveikumo programos viešųjų raktų katalogais (angl. PKD *Public Key Directory*);

12.3. sudaro sąlygas SVDPT vartotojų tapatumo nustatymo serveriui keistis duomenimis su Sąveikumo programos tinklų vartotojų tapatumo nustatymo serveriais.

13. SVDPT, įgyvendindamas 4.2 uždavinį, atlieka šias funkcijas:

13.1. teikia visą šalį apimantį telematinį elektroninių ryšių tinklą ir visą su šiuo tinklu susijusią informacinių ir ryšių technologijų infrastruktūrą;

13.2. teikia Lietuvos Respublikos institucijoms aukštos greitaveikos plačiajuostį ryšį multimedijos paslaugoms;

13.3. sudaro Lietuvos Respublikos institucijoms saugaus ryšio su viešaisiais duomenų perdavimo tinklais sąlygas;

13.4. sudaro saugaus duomenų perdavimo Lietuvos Respublikos institucijų informacinėms sistemoms ir žinybiniams ryšio tinklams sąlygas;

13.5. sudaro sąlygas užtikrinti registrų bei valstybės informacinių sistemų saugą.

14. SVDPT, įgyvendindamas 4.3 uždavinį, atlieka šias funkcijas:

14.1. teikia uždaro tarnybinio laidinio ir belaidžio telefono ryšio paslaugas Lietuvos Respublikos institucijoms;

14.2. sudaro sąlygas informacijos apie atvirųjų programų naudojimo patirtį Europos Sąjungos valstybėse narėse bei šių programų pritaikymą ir platinimą Lietuvos Respublikos institucijose sklaidai;

15. SVDPT, įgyvendindamas 4.4 uždavinį, atlieka šias funkcijas:

15.1. teikia Lietuvos Respublikos e. valdžios pagrindinio portalo prieglobą ir užtikrina jo apsaugą;

15.2. teikia Lietuvos Respublikos institucijų oficialių tinklalapių prieglobą ir užtikrina jo apsaugą;

15.3. sudaro sąlygas fizinių ir juridinių asmenų tapatumo nustatymui teikiant jiems Lietuvos Respublikos e. valdžios paslaugas;

16. SVDPT, įgyvendindamas 4.5 uždavinį, atlieka šias funkcijas

16.1. teikia saugaus tarnybinio elektroninio pašto paslaugas Lietuvos Respublikos institucijoms ryšiams su Europos Sąjungos institucijomis ir valstybių narių administracijomis ir tarpusavyje;

16.2. teikia Lietuvos Respublikos institucijoms viešųjų raktų katalogų (PKD) paslaugas uždaroms vartotojų grupėms;

16.3. sudaro registrų ir valstybės informacinių sistemų duomenų saugaus informacijos perdavimo Lietuvos Respublikos institucijoms paslaugas:

16.3.1. Valstybės įmonės „Registrų centras“ registrų saugų keitimąsi duomenimis su kitais valstybės registrais;

16.3.2. Valstybinės reikšmės ir pavojingų objektų registro informacijos saugų perdavimą Lietuvos Respublikos institucijoms;

16.3.3. duomenų apie registruotas transporto priemones saugų perdavimą Lietuvos Respublikos institucijoms.

16.4. sudaro sąlygas saugiai ir operatyviai Europos Tarybos Generalinio sekretoriato siunčiamus dokumentus išplatinti Lietuvos Respublikos institucijoms;

16.5. sudaro sąlygas Lietuvos Respublikos institucijų valstybės tarnautojų ir darbuotojų, dirbančių pagal darbo sutartis, tapatumui nustatyti jiems naudojantis valstybinių informacinių sistemų ištekliais;

16.6. sudaro sąlygas naudotis Europos Sąjungos valstybių narių elektroninių vyriausybių paslaugomis:

16.6.1. teikia Lietuvos Respublikos dalyvavimo Sąveikumo programoje portalo prieglobą (angl. hosting) ir sudaro sąlygas ją administruoti;

16.6.2. sudaro sąlygas Europos Sąjungos valstybių narių e. valdžios paslaugų, teikiamų per TESTA ir kitus Sąveikumo programos paslaugų tinklus, teikti Lietuvos Respublikos fiziniams ir juridiniams asmenims.

IV SKYRIUS
SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO DUOMENŲ SAUGOS UŽTIKRINIMAS

17. SVDPT organizacinės ir techninės duomenų saugos priemonės, skirtos užtikrinti SVDPT ir juo perduodamų duomenų konfidencialumą, prieinamumą, vientisumą, įgyvendinamos vadovaujantis Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašu, patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. balandžio 20 d. nutarimu Nr. 387 „Dėl Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašo patvirtinimo“, Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu, ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašu, patvirtintais Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo ir elektroninės informacijos svarbos nustatymo gairių aprašo patvirtinimo“, bei Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimais (1 priedas).

18. Europos Sąjungos ir valstybių narių administracijų elektroninio keitimosi duomenimis saugos užtikrinimo priemonės yra įdiegtos Sąveikumo programos paslaugų tinkluose, o Lietuvos Respublikoje – SVDPT.

19. Elektroninio keitimosi duomenimis ir duomenų saugos užtikrinimo priemonės turi atitikti sutarties tarp Europos Bendrijos Sąveikumo programos komisijos ir Lietuvos Respublikos Vyriausybės įgaliotos institucijos sąlygas.

20. Siekiant padidinti SVDPT kamieninės dalies patikimumą, SVDPT tvarkytojas konkursu parenka ne mažiau kaip du telekomunikacijų paslaugų teikėjus.

V SKYRIUS
FINANSAVIMO ŠALTINIAI

21. SVDPT plėtra, modernizavimas ir priežiūra gali būti finansuojami Lietuvos Respublikos valstybės biudžeto lėšomis, Europos Sąjungos, SVDPT tvarkytojo ir kitomis teisėtai gautomis lėšomis.

VI SKYRIUS
SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO PASLAUGŲ TEIKIMO TVARKA IR ATLYGINIMO DYDŽIAI

22. SVDPT sujungtas su TESTA ir kitais Sąveikumo programos paslaugų tinklais. SVDPT valdymo centre įrengti vartai į Europos domeną – komunikacijų mazgas, jungiantis SVDPT (vietinį domeną) su visas Europos Sąjungos institucijas apimančiu telematiniu elektroninių ryšių tinklu – TESTA (Europos domenas).

23. TESTA ir kitų Sąveikumo programos tinklų paslaugos Lietuvos Respublikos institucijoms teikiamos SVDPT, vadovaujantis Elektroninio keitimosi duomenimis su Europos Sąjungos ir valstybių narių administracijomis taisyklėmis, patvirtintomis Lietuvos Respublikos

vidaus reikalų ministro 2004 m. vasario 24 d. įsakymu Nr. 1V-50 „Dėl Elektroninio keitimosi duomenimis su Europos Sąjungos ir valstybių narių administracijomis taisyklių patvirtinimo“.

24. Lietuvos Respublikos prisijungimo prie Sąveikumo programos tinklų sąlygos nustatomos sutartimi tarp Europos Bendrijos Sąveikumo programos komisijos ir Lietuvos Respublikos Vyriausybės įgaliotos institucijos. Šia sutartimi nustatomos sutartį pasirašiusių šalių teisės ir pareigos teikiant TESTA ir kitų Sąveikumo programos tinklų paslaugas bei užtikrinant šiais tinklais teikiamų paslaugų saugumą ir ryšio su Sąveikumo programos tinklais sąlygas.

25. SVDPT paslaugų teikimą nustato Saugaus valstybinio duomenų perdavimo tinklo paslaugų teikimo taisyklės (2 priedas). SVDPT paslaugų teikimo sąlygos nustatomos SVDPT paslaugų teikimo sutartyse su Lietuvos Respublikos institucijomis.

26. Atlyginimo už naudojimąsi SVDPT dydžius pagal Lietuvos Respublikos Vyriausybės patvirtintus kriterijus tvirtina Lietuvos Respublikos krašto apsaugos ministerija. SVDPT paslaugų kainos apskaičiuojamos pagal Lietuvos Respublikos krašto apsaugos ministro įsakymu patvirtintą paslaugų, teikiamų SVDPT, kainų apskaičiavimo metodiką.

_____

Saugaus valstybinio duomenų perdavimo
tinklo nuostatų
1 priedas

SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO ELEKTRONINĖS INFORMACIJOS SAUGOS REIKALAVIMAI

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimai (toliau – Saugos reikalavimai) tikslas yra nustatyti ir įgyvendinti organizacines, technines ir kitas priemones, sudarančias sąlygas saugiam elektroninės informacijos perdavimui, saugojimui ar apdorojimui Saugiame valstybiniame duomenų perdavimo tinkle (toliau – SVDPT).

2. Saugos reikalavimuose vartojamos sąvokos atitinka sąvokas, nustatytas Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“, Lietuvos standarte LST ISO/IEC 27001 ir kituose teisės aktuose, reglamentuojančiuose elektroninės informacijos saugą.

3. SVDPT perduodamos, saugomos ar kitaip apdorojamos elektroninės informacijos sauga yra vertinama pagal elektroninės informacijos konfidencialumą, prieinamumą, vientisumą ir transakcijų nepaneigiamumą – SVDPT savybę, parodančią, kad atitinkamus veiksmus SVDPT atlikę asmenys negali paneigti atlikę šiuos veiksmus.

4. SVDPT tvarkytojas naudoja formalizuotą elektroninės informacijos saugos valdymo sistemą, atitinkančią LST ISO/IEC 27001 standarto reikalavimus, kuri yra susieta bei suderinta su kitomis SVDPT tvarkytojo turimomis veiklos valdymo sistemomis, kuri užtikrina:

4.1. elektroninės informacijos saugos poreikio supratimą, įvertinimą bei tinkamų SVDPT elektroninės informacijos saugos politikos ir tikslų nustatymą;

4.2. elektroninės informacijos saugos rizikos valdymo poreikio supratimą, įvertinimą bei tinkamų rizikos valdymo ir kontrolės priemonių įdiegimą;

4.3. sistemingą elektroninės informacijos saugos stebėjimą, vertinimą ir tobulinimą.

II SKYRIUS
PAGRINDINĖS GRĖSMIŲ SVDPT SAUGAI GRUPĖS

5. Šiame skyriuje apibūdintos pagrindinės grėsmių SVDPT saugai grupės, kurios turi būti įvertinamos įgyvendinant saugos reikalavimus ir įdiegiant elektroninės informacijos saugos užtikrinimo priemones SVDPT. Detalus grėsmių, darančių įtaką SVDPT ir elektroninės informacijos saugai, įvertinimas turi būti atliekamas periodinės SVDPT saugos rizikos analizės metu.

6. Loginio pobūdžio grėsmės, kylančios dėl:

6.1. Lietuvos Respublikos valstybės ir savivaldybių institucijų, įstaigų ir įmonių, kurios yra sudariusios SVDPT paslaugų teikimo sutartį (toliau – SVDPT naudotojai) apsimetimo kitais SVDPT naudotojais;

6.2. SVDPT tvarkytojo darbuotojų, dirbančių pagal darbo sutartis (toliau – SVDPT tvarkytojo darbuotojai), ar rangovų apsimetimo SVDPT naudotojų valstybės tarnautojais ir darbuotojais, dirbančiais pagal darbo sutartis (toliau – SVDPT naudotojų darbuotojai);

6.3. pašalinių asmenų apsimetimo SVDPT naudotojų darbuotojais;

6.4. SVDPT tvarkytojo darbuotojų ir SVDPT naudotojų darbuotojų neleistinos SVDPT

programinės įrangos naudojimo;

6.5. pašalinių asmenų, nesudariusių SVDPT paslaugų teikimo sutarties, prijungimo prie SVDPT;

6.6. kenksmingojo programinio kodo įdiegimo į ryšių tinklus, techninę, programinę, komunikacinę įrangą, sudarančią SVDPT ir užtikrinančią SVDPT paslaugų teikimą (toliau – SVDPT informaciniai ištekliai);

6.7. SVDPT tvarkytojo darbuotojų ir SVDPT naudotojų darbuotojų prieigos prie SVDPT informacinių išteklių ir elektroninės informacijos asmeniniais tikslais;

6.8. kitų priežasčių.

7. Komunikacinės grėsmės, kylančios dėl:

7.1. įsiskverbimo į SVDPT informacinius išteklius, naudojant įvairias atakas, tokias kaip atminties perpildymas (angl. *buffer overflow*), apsimetimas tarnybine stotimi, atsisakymas teikti paslaugas (angl. *denial of Service*);

7.2. įsiskverbimo į SVDPT naudotojų tinklus ir SVDPT informacinius išteklius siunčiant nepageidaujamas elektroninio pašto žinutes (angl. *spam*) iš atviրųjų tinklų;

7.3. SVDPT perduodamos elektroninės informacijos perėmimo, elektroninės informacijos gavimo laiko arba tvarkos sutrikdymo, elektroninės informacijos gavėjo pakeitimo;

7.4. manipuliavimo elektronine informacija ir SVDPT atliktų veiksmų neigimo ar išsižadėjimo;

7.5. neteisingo duomenų srautų maršruto parinkimo ar duomenų srautų nukreipimo;

7.6. ryšio linijų sutrikimų;

7.7. kitų priežasčių.

8. Techninių sutrikimų grėsmės, kylančios dėl:

8.1. techninių SVDPT tarnybinių stočių sutrikimų;

8.2. vartų į Europos domeną ir vartų į SVDPT techninių įrenginių sutrikimų;

8.3. techninių elektroninės informacijos saugos valdymo sistemos sutrikimų;

8.4. techninių elektroninės informacijos saugojimo įrenginių sutrikimų;

8.5. techninių SVDPT komutavimo įrenginių sutrikimų;

8.6. techninių elektroninės informacijos perdavimo įrenginių sutrikimų;

8.7. techninių prieigos prie SVDPT informacinių išteklių ir elektroninės informacijos įrenginių sutrikimų;

8.8. techninių SVDPT funkcinių sistemų valdymo įrenginių sutrikimų;

8.9. techninių SVDPT infrastruktūros įrenginių (maitinimo šaltinių, oro kondicionavimo, ventiliacijos sistemų) sutrikimų;

8.10. kitų priežasčių.

9. Žmonių klaidų grėsmės, kylančios dėl:

9.1. klaidų, padarytų SVDPT tvarkytojo darbuotojų eksploatuojant SVDPT įrangą ir teikiant SVDPT paslaugas, kurias SVDPT tvarkytojas teikia SVDPT naudotojams per SVDPT ir kurių sąrašas yra pateikiamas Saugaus valstybinio duomenų perdavimo tinklo paslaugų teikimo taisyklėse (toliau – SVDPT paslaugos);

9.2. klaidų, padarytų SVDPT naudotojų darbuotojų prižiūrint vartus į SVDPT;

9.3. klaidų, padarytų SVDPT naudotojų darbuotojų dirbant su SVDPT veikiančiomis informacinėmis sistemomis ir taikomosiomis programomis;

9.4. klaidų, padarytų SVDPT naudotojų darbuotojų prižiūrint SVDPT naudotojų tinklus, techninę ir programinę įrangą;

9.5. kitų priežasčių.

10. Fizinio pažeidimo grėsmės, kylančios dėl:

10.1. gaisro;

10.2. vandens ir nuotekų išsiliejimo;

10.3. ekstremalių įvykių ir žmogaus veiklos sukeltų nelaimingų įvykių;

10.4. SVDPT tvarkytojo darbuotojų stokos;

10.5. SVDPT informacinių išteklių vagysčių, įvykdytų SVDPT tvarkytojo darbuotojų,

SVDPT naudotojų darbuotojų ar pašalinių asmenų;

10.6. SVDPT informaciniams ištekliams SVDPT tvarkytojo darbuotojų, SVDPT naudotojų darbuotojų ar pašalinių asmenų padarytos tyčinės žalos;

10.7. terorizmo;

10.8. kitų priežasčių.

III SKYRIUS
ELEKTRONINĖS INFORMACIJOS SAUGOS ORGANIZAVIMAS IR VALDYMAS

11. SVDPT tvarkytojas įgyvendina SVDPT elektroninės informacijos saugą ir atsako už SVDPT informacinių išteklių saugą.

12. SVDPT tvarkytojas, atsižvelgdamas į ISO/IEC 18028 standarto reikalavimus, IETF RFC 2196 ir RFC 2411 rekomendacijas, Saugaus valstybinio duomenų perdavimo tinklo nuostatus, Saugaus valstybinio duomenų perdavimo tinklo paslaugų teikimo taisykles, saugos reikalavimus ir SVDPT tvarkytojo organizuotos SVDPT rizikos analizės rezultatus, turi:

12.1. nustatyti SVDPT saugos architektūrą;

12.2. nustatyti ir įdiegti saugaus SVDPT paslaugų teikimo priemones;

12.3. nustatyti ir įdiegti SVDPT eksploatavimo ir priežiūros priemones;

12.4. nustatyti ir įdiegti SVDPT naudotojų identifikavimo ir autentifikavimo priemones;

12.5. nustatyti ir įdiegti SVDPT vykdomų veiksmų apskaitos ir audito priemones;

12.6. nustatyti ir įdiegti piktybinės veiklos (įsilaužimų) nustatymo ir apsaugos nuo kenksmingojo programinio kodo programų priemones;

12.7. nustatyti ir įdiegti elektroninės informacijos šifravimo priemones;

12.8. nustatyti ir įdiegti atsarginių elektroninės informacijos kopijų darymo, saugojimų ir elektroninės informacijos atkūrimo iš atsarginių elektroninės informacijos kopijų priemones;

12.9. nustatyti ir įdiegti SVDPT veiklos tęstinumo užtikrinimo priemones.

13. SVDPT tvarkytojas turi užtikrinti, kad visos SVDPT perduodamos, saugomos ar kitaip apdorojamos įslaptintos informacijos konfidencialumo lygis atitiktų Lietuvos Respublikos teisės aktais nustatytus reikalavimus, keliamus įslaptintai informacijai, pažymėtai slaptumo žyma „Riboto naudojimo“, ir Europos Sąjungos teisės aktais nustatytus reikalavimus, keliamus įslaptintai informacijai, pažymėtai slaptumo žyma RESTREINT UE. Taip pat turi būti užtikrintos sąlygos, būtinos asmens duomenims ir valstybės institucijų valdomų informacinių sistemų, valstybės ir žinybinių registrų elektroninei informacijai perduoti.

14. Konkretus elektroninės informacijos konfidencialumo lygis nustatomas SVDPT paslaugų teikimo sutartyse.

15. Elektroninė informacija apie SVDPT, SVDPT informacinius išteklius, SVDPT veiklą klasifikuojama pagal SVDPT tvarkytojo vadovo nustatytą tvarką, kuri turi būti privaloma visiems SVDPT tvarkytojo darbuotojams.

16. SVDPT tvarkytojo paskirtas saugos įgaliotinis (toliau – SVDPT saugos įgaliotinis) yra atsakingas už elektroninės informacijos saugos įgyvendinimą SVDPT. SVDPT saugos įgaliotinis vykdo funkcijas, numatytas Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Bendrieji saugos reikalavimai), ir kitus SVDPT tvarkytojo nurodymus.

17. SVDPT tvarkytojo paskirtas saugos administratorius (toliau – SVDPT saugos administratorius) yra atsakingas už SVDPT saugos priemonių įdiegimą ir priežiūrą. SVDPT saugos administratorius vykdo funkcijas, numatytas Bendruosiuose saugos reikalavimuose, šiuose saugos reikalavimuose ir kitus SVDPT tvarkytojo nurodymus.

18. Elektroninės informacijos saugą, pagal SVDPT paslaugų teikimo sutartis, SVDPT

naudotojų tinklų dalyse, sujungtose su SVDPT, turi įgyvendinti SVDPT naudotojai.

19. SVDPT naudotojai turi paskirti saugos įgaliotinius, atsakingus už SVDPT naudotojų tinklų dalių, sujungtų su SVDPT, saugos įgyvendinimą.

20. SVDPT paslaugos gali būti teikiamos tik pagal SVDPT paslaugų teikimo sutartis. Prieš pasirašant SVDPT paslaugų teikimo sutartis ir jei SVDPT paslaugų teikimo sutarčių galiojimo metu padaroma žymių pakeitimų SVDPT naudotojų tinkluose, SVDPT tvarkytojas, siekdamas išsiaiškinti galimą grėsmę SVDPT saugai ir SVDPT naudotojo pažeidžiamumą, gali organizuoti SVDPT naudotojo atitikimo saugos reikalavimams įvertinimą.

21. SVDPT paslaugų teikimo sutartyse turi būti nustatyta:

21.1. teikiamų SVDPT paslaugų aprašymas;

21.2. elektroninei informacijai taikytinas konfidencialumo lygis;

21.3. reikalavimas SVDPT naudotojui parengti elektroninės informacijos saugos politiką;

21.4. reikalavimas SVDPT naudotojui nustatyti SVDPT naudotojų darbuotojų, turinčių prieigos prie SVDPT informacinių išteklių ir elektroninės informacijos teisę, tapatybę;

21.5. SVDPT naudotojo tinklo prijungimo prie SVDPT įrangos ir SVDPT naudotojo darbuotojų darbo vietų fizinio saugumo reikalavimai;

21.6. SVDPT paslaugų ir elektroninės informacijos prieinamumo reikalavimai ir kriterijai;

21.7. SVDPT naudotojo tinklo ar jo dalies, prijungtos prie SVDPT, ribos;

21.8. SVDPT tvarkytojo ir SVDPT naudotojo atsakomybė už elektroninės informacijos saugą;

21.9. SVDPT tvarkytojo ir SVDPT naudotojų pareigos, susijusios su techninės ir programinės įrangos įdiegimu ir palaikymu SVDPT.

22. SVDPT tvarkytojo pareigos:

22.1. SVDPT naudotojams užtikrinti elektroninės informacijos prieinamumą. Per 1 mėnesį SVDPT paslaugų prieinamumas turi būti ne mažesnis nei 99,7 proc, o per 1 metus – 99,9 proc.;

22.2. užtikrinti, kad bet koks SVDPT saugomos, perduodamos ar kitaip apdorojamos elektroninės informacijos, kuri pagal elektroninės informacijos savininko sprendimą turi būti prieinama tik atitinkamiems SVDPT naudotojams, atskleidimas pašaliniams asmenims, pažeidžiant SVDPT paslaugų teikimo sutartį, nebūtų leistinas. Konkretūs SVDPT paslaugų ir elektroninės informacijos prieinamumo reikalavimai ir kriterijai turi būti nustatomi SVDPT paslaugų teikimo sutartyje;

22.3. užtikrinti, kad SVDPT paslaugų teikimas būtų kontroliuojamas ir valdomas atsižvelgiant į tiesiogines grėsmes elektroninės informacijos vientisumui SVDPT, o įvykus elektroninės informacijos vientisumo pažeidimui, elektroninės informacijos vientisumas būtų kuo skubiau atkurtas naudojant saugias atsargines elektroninės informacijos kopijas;

22.4. užtikrinti, kad nebūtų sudarytos sąlygos sutrikdyti transakcijų nepaneigiamumą. Konkretūs SVDPT transakcijų nepaneigiamumo kriterijai turi būti nustatomi SVDPT paslaugų teikimo sutartyse.

IV SKYRIUS
REIKALAVIMAI PERSONALUI

23. SVDPT tvarkytojo darbuotojų ir SVDPT naudotojų darbuotojų pareiginėse instrukcijose ir pareigybių aprašymuose turi būti numatytos jų funkcijos užtikrinant elektroninės informacijos ir SVDPT saugą.

24. SVDPT tvarkytojo darbuotojai, SVDPT naudotojų darbuotojai, rangovai su SVDPT tvarkytoju turi pasirašyti konfidencialumo sutartis, užtikrinančias, kad jokia įslaptinta informacija ar elektroninė informacija, gauta iš SVDPT tvarkytojo, nebus atskleista trečiosioms šalims.

25. SVDPT tvarkytojas turi sukurti ir įgyvendinti procedūras, užtikrinančias, kad SVDPT tvarkytojo darbuotojams ar SVDPT naudotojų darbuotojams palikus darbą, rangovams baigus vykdyti savo įsipareigojimus apie tai būtų informuojami už SDVPT tvarkytojo ar SVDPT naudotojų patalpų fizinę saugą atsakingi asmenys (budėtojai), panaikintos SVDPT tvarkytojo darbuotojams,

SVDPT naudotojų darbuotojams, rangovams suteiktos prieigos prie SVDPT informacinių išteklių ir elektroninės informacijos teisės.

26. SVDPT tvarkytojo darbuotojai ir SVDPT naudotojų darbuotojai prieš pradėdami darbą su SVDPT turi būti supažindinti su SVDPT ir prie SVDPT prijungtų SVDPT naudotojų tinklų saugą reglamentuojančiais teisės aktais, taip pat rekomenduojama jiems suteikti elektroninės informacijos saugos pradmenis.

27. SVDPT tvarkytojo darbuotojai ir SVDPT naudotojų darbuotojai, kurių funkcijos tiesiogiai susijusios su SVDPT ir prie SVDPT prijungtų tinklų saugos užtikrinimu, turi nuolatos kelti savo kvalifikaciją elektroninės informacijos saugos užtikrinimo srityje.

28. Vienas SVDPT tvarkytojo saugos administratorius gali administruoti ne daugiau kaip vieną SVDPT sudėtinę dalį.

V SKYRIUS
REIKALAVIMAI ATPAŽINTIES PRIEMONĖMS

29. SVDPT tvarkytojas turi užtikrinti prie SVDPT prijungtos techninės įrangos atpažinimą ir prisijungusių asmenų tapatybės nustatymą.

30. Techninės įrangos atpažinimo tikslas yra užtikrinti, kad prieiga prie SVDPT informacinių išteklių ir elektroninės informacijos būtų galima tik iš tam tikros SVDPT paslaugų teikimo sutartyse numatytos techninės įrangos. Techninės įrangos atpažinimui turi būti naudojamos įrangos atpažinimo žymos, viešųjų raktų infrastruktūra.

31. Asmenų tapatybės nustatymo tikslas yra užtikrinti, kad prieiga prie SVDPT informacinių išteklių ir elektroninės informacijos būtų galima tik tam tikriems, SVDPT paslaugų teikimo sutartyse numatytiems asmenims. Asmenų tapatybės nustatymui turi būti naudojami vardai, slaptažodžiai, viešųjų raktų infrastruktūra.

32. Visų prieigos prie SVDPT informacinių išteklių ir elektroninės informacijos teisių ir priemonių suteikimas, pakeitimas ar panaikinimas SVDPT tvarkytojo darbuotojams ir SVDPT naudotojų darbuotojams turi būti registruojamas SVDPT tvarkytojo vadovo nustatyta tvarka.

VI SKYRIUS
REIKALAVIMAI PATALPŲ IR APLINKOS SAUGUMUI

33. Patekimas į pastatus ir patalpas, kuriuose yra SVDPT tvarkytojui priklausantys SVDPT informaciniai ištekliai, turi būti vykdomas vadovaujantis SVDPT tvarkytojo nustatyta tvarka, kurioje turi būti įtvirtintos šios nuostatos:

33.1. patekimas į pastatus ir patalpas, kuriuose yra SVDPT tvarkytojui priklausantys SVDPT informaciniai ištekliai, turi būti kontroliuojamas fizinėmis ir techninėmis prieigos kontrolės priemonėmis;

33.2. asmenys, patenkantys į pastatus ir patalpas, kuriuose yra SVDPT tvarkytojui priklausantys SVDPT informaciniai ištekliai, turi būti identifikuojami;

33.3. turi būti kaupiama informacija apie asmens patekimo į pastatus ir patalpas, kuriuose yra SVDPT tvarkytojui priklausantys SVDPT informaciniai ištekliai, datą ir laiką;

33.4. visi asmenys, esantys pastatuose ir patalpose, kuriuose yra SVDPT tvarkytojui priklausantys SVDPT informaciniai ištekliai, visą laiką turi segėti tapatybę patvirtinančias korteles arba svečių leidimus;

33.5. visos kompiuterinės, telekomunikacinės įrangos ir informacinių laikmenų įnešimas arba išnešimas iš patalpų, kuriose yra SVDPT tvarkytojui priklausantys SVDPT informaciniai ištekliai, turi būti vykdomas tik SVDPT tvarkytojo vadovo įgaliotų asmenų.

34. Turi būti užtikrinta, kad pastatai ir patalpos, kuriuose yra SVDPT tvarkytojui priklausantys SVDPT informaciniai ištekliai:

34.1. būtų apsaugoti įsilaužimų aptikimo sistema, kurios nuolatinis veikimas būtų užtikrintas naudojant nepertraukiamus maitinimo šaltinius;

34.2. atitiktų priešgaisrinės apsaugos reikalavimus;

34.3. būtų tikrinami periodiškai ir įtarus, kad į juos buvo įsibrauta.

VII SKYRIUS
REIKALAVIMAI PROGRAMINĖS ĮRANGOS SAUGOS PRIEMONĖMS

35. Siekiant apsaugoti SVDPT saugomą, perduodamą ar kitaip apdorojamą elektroninę informaciją, būtina SVDPT įdiegti elektroninės informacijos šifravimo, apsaugos nuo kenksmingojo programinio kodo ir SVDPT naudotojų saugaus prijungimo prie SVDPT priemones.

36. SVDPT turi būti suskaidytas į SVDPT sritis, kurios fiziškai ir / arba logiškai būtų atskirtos tarpusavyje ir nuo kitų tinklų ir atitiktų bendrus tai SVDPT sričiai keliamus elektroninės informacijos saugos reikalavimus. Įslaptinta informacija ir viešam naudojimui neskirta elektroninė informacija gali būti perduodama tik šifruotu pavidalu ir negali būti prieinama kitų SVDPT sričių SVDPT naudotojams. Viešoji elektroninė informacija SVDPT gali būti perduodama nešifruota.

37. SVDPT turi būti įdiegtos priemonės, užtikrinančios, kad:

37.1. elektroninė informacija perdavimo metu nebūtų pakeista;

37.2. būtų patvirtinta elektroninės informacijos siuntėjo ir gavėjo tapatybė;

37.3. elektroninė informacija perdavimo metu nebūtų perimta.

38. Turi būti įdiegtos ir nuolatos atnaujinamos apsaugos priemonės (antivirusinė programinė įranga) nuo kenkėjiškos programinės įrangos (kompiuterinių virusų, „Trojos arklių“) ir:

38.1. privaloma laikytis programinės įrangos licencijose nustatytų nurodymų;

38.2. draudžiama naudoti nelicencijuotą programinę įrangą;

38.3. nelegali programinė įranga turi būti šalinama ir nustatomas jos atsiradimo šaltinis;

38.4. elektroninės informacijos laikmenos prieš jas naudojant SVDPT turi būti patikrintos, ar jose nėra kenkėjiškos programinės įrangos.

39. SVDPT naudojamos užkardos turi atitikti EAL4 lygį pagal standartą ISO/IEC 15408 ir turi būti naudojamos pagal šio standarto reikalavimus. Periodiškai turi būti peržiūrimi užkardų įrašai siekiant įvertinti bandymus sutrikdyti SVDPT veiklą.

VIII SKYRIUS
REIKALAVIMAI NAUDOTOJŲ PRISIJUNGIMUI

40. SVDPT naudotojų saugus prijungimas prie SVDPT turi būti užtikrintas įgyvendinant šiuos reikalavimus:

40.1. SVDPT naudotojų tinklų tarnybinės stotys, SVDPT naudotojų darbo vietos ir kita įranga, siunčianti ir gaunanti elektroninę informaciją per SVDPT, turi turėti fiksuotus vidinius IP adresus SVDPT naudotojo tinkle;

40.2. SVDPT naudotojų tinklo prijungimai prie viešųjų ryšio tinklų turi būti atliekami per vieną koncentruojantį įrenginį ir apsaugoti užkarda;

40.3. SVDPT naudotojų mobiliųjų darbo vietų prijungimai prie SVDPT naudotojų tinklų turi būti realizuoti naudojant atskirus SVDPT naudotojų virtualius tinklus; šie prijungimai turi būti atliekami per vieną koncentruojantį įrenginį ir apsaugoti užkarda;

40.4. SVDPT naudotojų tinklų dalis, prijungta prie SVDPT, negali turėti tiesioginių ryšių su mobiliosiomis darbo vietomis, išskyrus ryšį per specialias apsaugotas SVDPT sritis;

40.5. SVDPT naudotojų tinklų dalis, turinti ryšį su SVDPT, neturi turėti tiesioginių (naudojant tinklo adresų transliaciją – NAT) ryšių su viešųjų ryšių tinklais;

40.6. SVDPT naudotojų tinklų dalis, turinti ryšį su bet kuria SVDPT sritimi, neturi turėti bevielio vietinio tinklo (angl. *wireless LAN*) prijungimo taškų;

40.7. SVDPT naudotojų tinklų dalis, turinti ryšį su bet kuria SVDPT sritimi, neturi turėti nuolatinių ar laikinų ryšio priemonių, skirtų nuotolinei SVDPT naudotojų tinklų priežiūrai ir konfigūravimui, pasiekiamų iš trečiųjų šalių darbo vietų be tam tikrų rašytinių susitarimų dėl tokių ryšio priemonių naudojimo ir elektroninės informacijos saugos.

41. Atsižvelgiant į tai, kad SVDPT naudotojai turi skirtingą SVDPT paslaugų poreikį, jų prijungimui prie SVDPT turi būti naudojami skirtingi prijungimo būdai:

41.1. Pirmasis būdas. Šis prijungimo būdas taikomas tuomet, kai prie SVDPT prijungiamas vietinis vienalytis (neturintis potinklių) SVDPT naudotojo tinklas, kuriuo elektroninė informacija teikiama kitiems SVDPT naudotojams, o prieiga prie viešųjų ryšių tinklų yra suteikiama per SVDPT. Tokiu būdu SVDPT naudotojai SVDPT paslaugas ir viešųjų ryšių tinklų išteklius pasiekia per skirtingas SVDPT sritis. Pirmojo būdo prijungimo schema pateikta saugos reikalavimų 1 priede.

41.2. Antrasis būdas. Šis prijungimo būdas taikomas tuomet, kai prieiga prie SVDPT paslaugų būtina tik kelioms SVDPT naudotojo darbuotojų darbo vietoms, o likusiai SVDPT naudotojo tinklo daliai būtina prieiga tik prie viešųjų ryšių tinklų, kuri užtikrinama ne per SVDPT Antrojo būdo prijungimo schema pateikta saugos reikalavimų 2 priede.

41.3. Trečiasis būdas. Šis prijungimo būdas taikomas tuomet, kai prie SVDPT prijungiamas regioninis nevienalytis (suskaidytas į potinklius) SVDPT naudotojo tinklas. SVDPT naudotojo tinklo nevienalytiškumas pasireiškia tuo, kad atskiroms jo dalims turi būti taikomi skirtingi saugos reikalavimai (daliai SVDPT naudotojo informacinių sistemų būtinas ryšis su viešųjų ryšių tinklais, daliai – su SVDPT paslaugomis), tačiau atskiras SVDPT naudotojo tinklo dalis sieja tos pačios informacinės sistemos. Dėl tokio SVDPT naudotojo tinklo nevienalytiškumo kyla tiesioginė grėsmė SVDPT perduodamos elektroninės informacijos saugai, todėl būtina SVDPT naudotojo tinklą suskaidyti į bendrąjį ir saugų potinklį, tarp kurių elektroninės informacijos perdavimas būtų kontroliuojamas elektroninės informacijos turinio ir srauto kontrolės priemonėmis. Trečiojo būdo prijungimo schema pateikta saugos reikalavimų 3 priede.

41.4. Ketvirtasis būdas. Šis prijungimo būdas taikomas tuomet, kai prie SVDPT prijungiamas vietinis nevienalytis (suskaidytas į potinklius) SVDPT naudotojo tinklas. Daliai SVDPT naudotojo tinklo būtina prieiga prie įslaptintos informacijos, o daliai – prie viešųjų ryšių tinklų. Ketvirtojo būdo prijungimo schema pateikta saugos reikalavimų 4 priede.

42. SVDPT naudotojų prijungimas prie SVDPT turi būti atliekamas per vieną ar kelis vartus į SVDPT. Daugiau nei vienas SVDPT naudotojas gali būti prijungiamas prie vienų vartų į SVDPT tik tuo atveju, kai tai užtikrina SVDPT paslaugų kokybę ir didesnį elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo lygį.

43. Pirmasis ir ketvirtasis SVDPT naudotojų prijungimo būdai užtikrina didesnį elektroninės informacijos saugos lygį, antrasis ir trečiasis SVDPT naudotojų prijungimo prie SVDPT būdai yra laikytini laikinais ir esant galimybei turi būti pakeisti į pirmąjį ar ketvirtąjį SVDPT naudotojų prijungimo būdą. SVDPT naudotojui pasirinkus antrąjį ar trečiąjį prijungimo prie SVDPT būdą, SVDPT tvarkytojui turi būti pateiktas tokio sprendimo pagrindimas ir terminas, per kurį SVDPT naudotojas prie SVDPT bus prijungtas pirmuoju ar ketvirtuoju būdu.

IX SKYRIUS
REIKALAVIMAI NAUDOTOJŲ VEIKSMŲ REGISTRAVIMUI

44. Siekiant aptikti neleistinus SVDPT tvarkytojo darbuotojų ir SVDPT naudotojų darbuotojų veiksmus perduodant, keičiant, trinant ar modifikuojant elektroninę informaciją, pagal SVDPT tvarkytojo vadovo nustatytą tvarką, turi būti vykdoma SVDPT vykdytų veiksmų apskaita ir auditas.

45. Siekiant palengvinti neleistinų SVDPT tvarkytojo darbuotojų ir SVDPT naudotojų darbuotojų veiksmų tyrimą, būtina kaupti ir saugoti SVDPT vykdytų veiksmų žurnalus (angl. *log).* SVDPT vykdytų veiksmų žurnaluose turi būti pateikta bent ši informacija:

45.1. prijungtų prie SVDPT įrenginių ir prisijungusių SVDPT naudotojų darbuotojų identifikatoriai;

45.2. svarbių SVDPT vykdytų veiksmų, pavyzdžiui, SVDPT naudotojų darbuotojų prisijungimo ir atsijungimo, data, laikas ir kita su tuo susijusi informacija;

45.3. įrašai apie sėkmingus ir nesėkmingus prieigos prie SVDPT informacinių išteklių ir elektroninės informacijos mėginimus, SVDPT nustatymų pakeitimus, elektroninės informacijos

pakeitimą;

45.4. įrašai apie SVDPT naudotojų darbuotojų prieigos prie SVDPT informacinių išteklių ir elektroninės informacijos teisių pakeitimus;

45.5. įrašai apie elektroninės informacijos saugos incidentus, SVDPT valdymo sistemos ar kitų SVDPT saugą užtikrinančių sistemų pavojaus signalus.

46. Kadangi SVDPT vykdytų veiksmų žurnaluose gali būti kaupiama įslaptinta informacija, būtina užtikrinti SVDPT vykdytų veiksmų žurnalų saugą atsižvelgiant į tokiai informacijai keliamus saugos reikalavimus.

47. Turi būti taikomas toks SVDPT vykdytų veiksmų registravimas, kuris leistų užtikrinti SVDPT transakcijų nepaneigiamumą.

X SKYRIUS
REIKALAVIMAI POKYČIŲ IR INCIDENTŲ VALDYMUI

48. SVDPT tvarkytojo vadovas turi nustatyti SVDPT daromų pakeitimų kontrolės tvarką, kad:

48.1. dėl kiekvieno SVDPT daromo pakeitimo turi būti gaunamas SVDPT tvarkytojo vadovo ar jo įgalioto asmens pritarimas;

48.2. SVDPT daromi pakeitimai turi būti planuojami, o jų įgyvendinimas tikrinamas;

48.3. planuojant SVDPT pakeitimus turi būti atliekamas pakeitimų poveikio SVDPT veiklai (įskaitant ir elektroninės informacijos saugą) įvertinimas;

48.4. nepavykus įgyvendinti SVDPT pakeitimo, turi būti imtasi atkūrimo (angl. *rollback)* veiksmų.

49. SVDPT techninės, programinės ir komunikacinės įrangos nustatymai, parametrai ir konfigūracija turi būti valdomi pagal SVDPT tvarkytojo vadovo patvirtintas procedūras. SVDPT techninės, programinės ir komunikacinės įrangos nustatymų, parametrų ir konfigūracijos valdymo procesas turi būti planuojamas, o jo įgyvendinimas tikrinimas (audituojamas). Planuojant SVDPT techninės, programinės ir komunikacinės įrangos nustatymų, parametrų ir konfigūracijos valdymo procesą, turi būti įvertinama šio proceso įtaka SVDPT veiklai (įskaitant ir elektroninės informacijos saugą).

50. SVDPT tvarkytojo vadovas turi nustatyti elektroninės informacijos saugos incidentų tyrimo tvarką – reglamentuoti elektroninės informacijos saugos incidentų, susijusių su SVDPT, SVDPT tvarkytojo veikla ir SVDPT paslaugų teikimu, registravimą, klasifikavimą, tyrimą, reagavimą į elektroninės informacijos saugos incidentus.

XI SKYRIUS
REIKALAVIMAI ATITIKTIES SAUGOS REIKALAVIMAMS VERTINIMUI IR RIZIKOS VERTINIMUI

51. Siekdamas užtikrinti SVDPT atitikimą saugos reikalavimams ir galimų grėsmių elektroninės informacijos saugai įvertinimą, SVDPT tvarkytojas privalo organizuoti SVDPT saugos rizikos analizę šiais atvejais:

51.1. periodiškai, ne rečiau kaip kartą per metus;

51.2. atliekant SVDPT, atskirų jo struktūrinių dalių, funkcinių sistemų keitimus, plėtrą ir naujų SVDPT paslaugų kūrimą;

51.3. kitais SVDPT tvarkytojo vadovo nustatytais atvejais.

52. Vykdant SVDPT saugos rizikos analizę taip pat turi būti atliekamas SVDPT informacinių išteklių pažeidžiamumo įvertinimas (angl. *penetration test*).

53. SVDPT tvarkytojas, atlikęs saugos reikalavimų 51 ir 52 punktuose numatytus darbus, turi parengti SVDPT saugos rizikos analizės ataskaitą, kuri turi būti pateikiama Lietuvos Respublikos krašto apsaugos ministerijai.

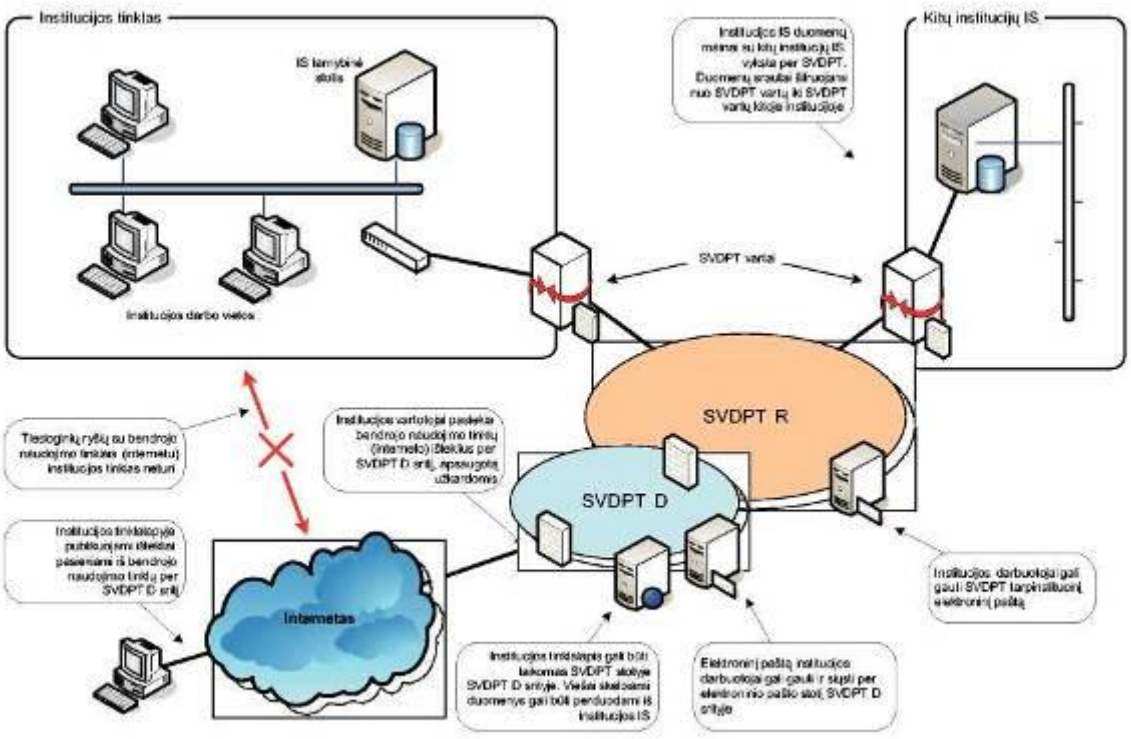
54. Siekdamas sumažinti neigiamą galimų SVDPT veiklos sutrikimų poveikį, SVDPT

tvarkytojo vadovas turi patvirtinti SVDPT veiklos tęstinumo valdymo planą, kurio veiksmingumas turi būti išbandomas ne rečiau kaip kartą per metus.

_____

Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimų
1 priedas

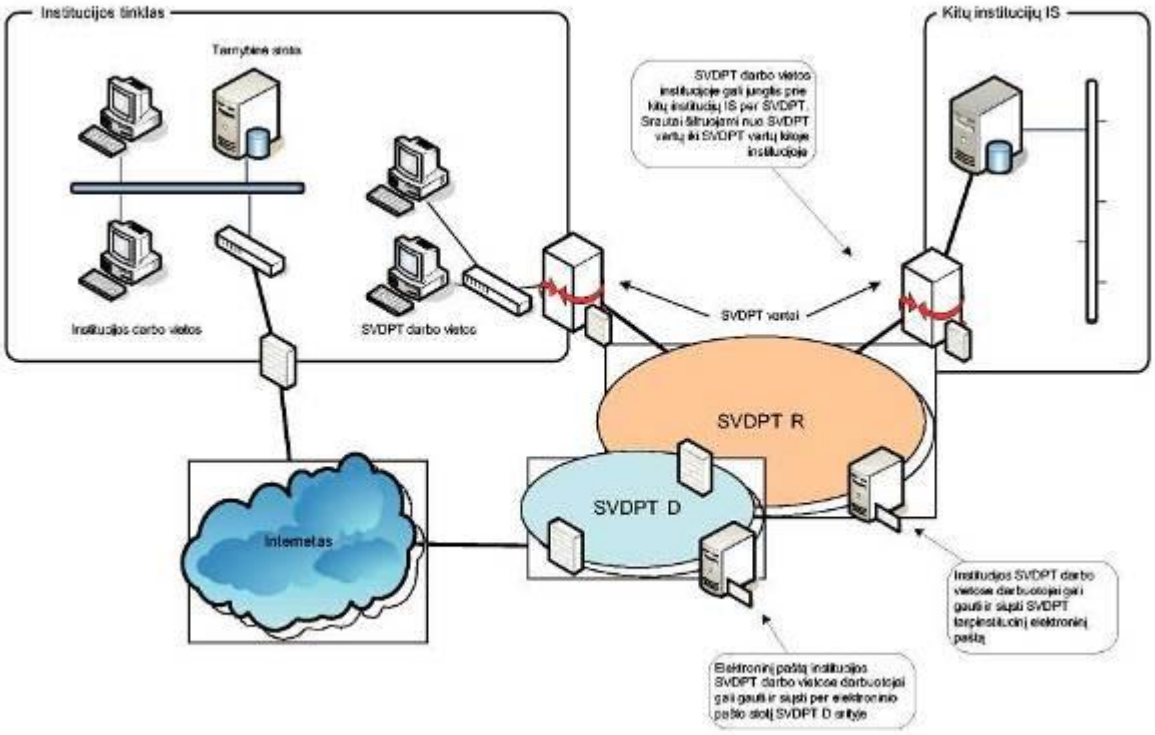
PRIJUNGIMO PRIE SVDPT PIRMASIS BŪDAS



_____

Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimų
2 priedas

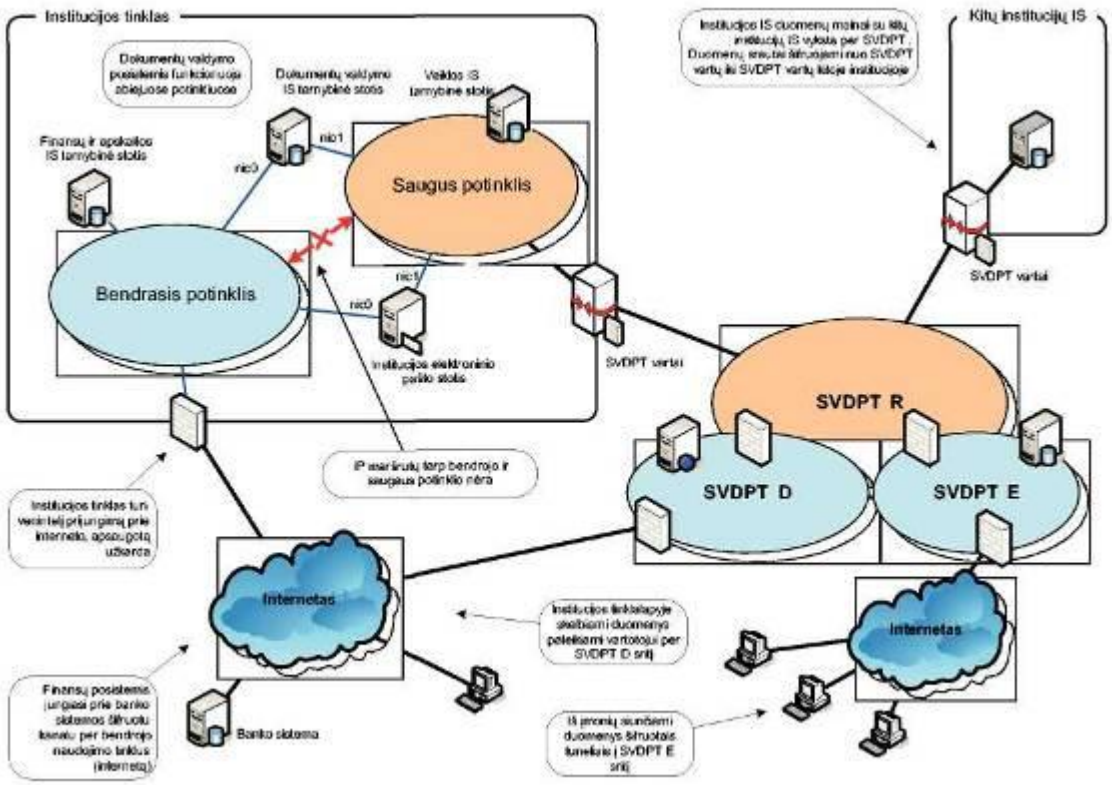
PRIJUNGIMO PRIE SVDPT ANTRASIS BŪDAS



_____

Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimų
3 priedas

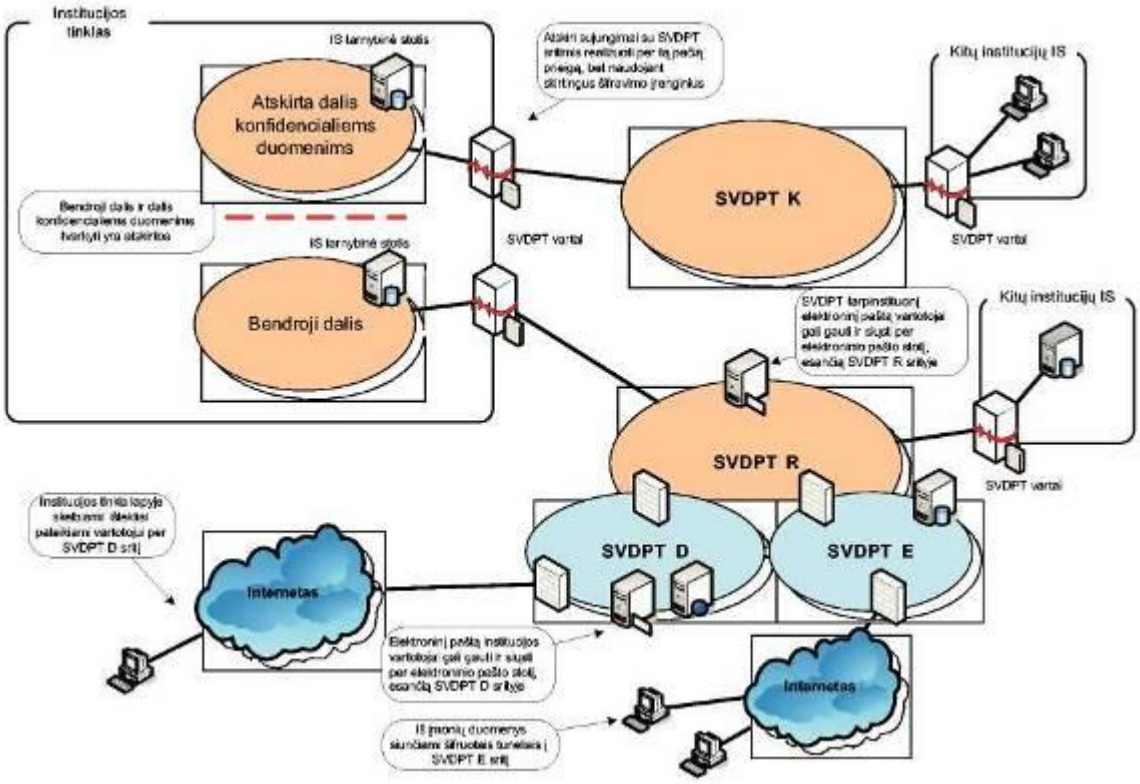
PRIJUNGIMO PRIE SVDPT TREČIASIS BŪDAS



_____

Saugaus valstybinio duomenų perdavimo tinklo elektroninės informacijos saugos reikalavimų
4 priedas

PRIJUNGIMO PRIE SVDPT KETVIRTASIS BŪDAS



_____

Saugaus valstybinio duomenų perdavimo tinklo nuostatų
2 priedas

SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO PASLAUGŲ TEIKIMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Saugaus valstybinio duomenų perdavimo tinklo paslaugų teikimo taisyklės (toliau – Taisyklės) reglamentuoja prijungimo prie Saugaus valstybinio duomenų perdavimo tinklo (toliau – SVDPT) ir jo paslaugų teikimo tvarką.

2. SVDPT teikiamomis paslaugomis gali naudotis Lietuvos Respublikos valstybės ir savivaldybių institucijos, įstaigos ir įmonės bei kiti asmenys, vykdantys valstybės priskirtas funkcijas (toliau – institucijos).

3. Taisyklės privalomos visoms Lietuvos Respublikos institucijoms, kurios yra prijungtos prie SVDPT ir naudojasi šiuo tinklu teikiamomis paslaugomis.

4. SVDPT draudžiama:

4.1. pažeisti SVDPT saugos tvarką, perduodamos ir apdorojamos informacijos konfidencialumą, vientisumą ir SVDPT komponentų ar teikiamų paslaugų prieinamumą (prieigos teisių pakeitimas, informacijos iškraipymas, informacijos viešinimas, nesankcionuotas naudojimasis paslaugomis, SVDPT ir Lietuvos Respublikos institucijų vietinių kompiuterių tinklų veikimo trikdymas, prievadų žvalgymas ir kt.);

4.2. dėti ir platinti kompiuterių programas ir kitus autorinius produktus nesilaikant licencijose nustatytų reikalavimų ar kitaip pažeidžiant autorių teises;

4.3. skelbti neoficialią informaciją;

4.4. dėti ir platinti reklaminę informaciją, išskyrus informaciją apie SVDPT teikiamas paslaugas;

4.5. užsiimti veikla, kuri pažeidžia Lietuvos Respublikos tarptautines sutartis, įstatymus, kitus galiojančius teisės aktus.

5. SVDPT privalu laikytis etiško paslaugų naudojimo principų, nustatytų Tarptautinės interneto standartizavimo organizacijos IETF (angl. „*The Internet Engineering Task Force*“) memorandumais RFC1087, RFC1855, ir kitose susijusiose rekomendacijose.

II SKYRIUS
LIETUVOS RESPUBLIKOS INSTITUCIJŲ JUNGIMAS PRIE SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO

6. Lietuvos Respublikos institucija, siekianti būti prijungta prie SVDPT ir naudotis jo paslaugomis, pateikia kvietimą dalyvauti pirkimo procedūrose (toliau – kvietimas) SVDPT tvarkytojui. Kartu su kvietimu pateikiamuose pirkimo dokumentuose turi būti nurodyta:

6.1. planuojami SVDPT paslaugų panaudojimo tikslai;

6.2. jungiamų prie SVDPT objektų adresai, ryšio kanalų greitaveikos ir prievadų tipai, gedimų šalinimo laikas ir kita informacija, reikalinga pasiūlymui paruošti;

6.3. atsakingo už prijungimą prie SVDPT Lietuvos Respublikos institucijos valstybės tarnautojo ar darbuotojo, dirbančio pagal darbo sutartį, kontaktiniai duomenys.

7. SVDPT tvarkytojas per vieną mėnesį nuo kvietimo ir pirkimo dokumentų pateikimo dienos įvertina Lietuvos Respublikos institucijos prijungimo prie SVDPT technines galimybes ir pateikia jai pasiūlymą, kuriame nurodo duomenų perdavimo ir saugumo užtikrinimo sąlygas, prijungimo prie SVDPT bei paslaugų teikimo sąmatą.

8. Lietuvos Respublikos institucijos prijungimo prie SVDPT techninis sprendimas ir prijungimo sparta parenkama atsižvelgiant į sąlygas, nurodytas kvietime.

9. SVDPT tvarkytojas su prijungiama Lietuvos Respublikos institucija sudaro SVDPT paslaugų teikimo sutartį, kurioje nustatomos prijungimo, paslaugų teikimo kainos ir atsiskaitymo už paslaugas sąlygos, šalių teisės ir pareigos teikiant SVDPT bei Europos viešojo administravimo institucijų, įskaitant vietos ir regionų viešojo administravimo institucijas, Europos Sąjungos institucijas ir organus, sąveikumo sprendimų programos, kuria užtikrinami bendrieji sąveikumą skatinantys sprendimai (toliau – Sąveikumo programa), tinklų paslaugas ir užtikrinant tų paslaugų saugumo ir ryšio teikimo sąlygas.

10. SVDPT tvarkytojas sutartyje su institucija nustatytomis sąlygomis įrengia, tvarko, prižiūri ir (ar) valdo SVDPT paslaugoms teikti naudojamą įrangą.

11. Paslaugomis besinaudojanti Lietuvos Respublikos institucija apmoka ryšio su SVDPT įrengimo, ryšio ir duomenų saugumo užtikrinimo įrangos, jos įrengimo bei paslaugų teikimo išlaidas.

12. Lietuvos Respublikos institucijai, iš esmės pažeidusiai SVDPT paslaugų teikimo sutarties sąlygas, laiku neatsiskaičiusiai už teikiamas paslaugas arba iš esmės pažeidusiai Taisyklių nuostatas ar atlikusiai veiksmus, kurie galėjo sukelti neigiamų padarinių SVDPT ir padaryti žalos jam ar kitoms prie jo prijungtoms Lietuvos Respublikos institucijoms, gali būti stabdomas paslaugų teikimas.

13. Dėl prie SVDPT prijungtos Lietuvos Respublikos institucijos kaltės padaryta turtinė ir neturtinė žala išieškoma Lietuvos Respublikos teisės aktų nustatyta tvarka.

III SKYRIUS
SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO PASLAUGŲ SĄRAŠAS IR KAINOS

14. SVDPT paslaugų sąrašą ir atlyginimo už naudojimąsi SVDPT paslaugomis dydžius pagal Lietuvos Respublikos Vyriausybės patvirtintus kriterijus tvirtina SVDPT valdytojas.

IV SKYRIUS
SAUGAUS VALSTYBINIO DUOMENŲ PERDAVIMO TINKLO PASLAUGOS

15. SVDPT yra sujungtas su TESTA (angl. Trans-European Services for Telematics between Administrations) ir kitais Sąveikumo programos tinklais ir teikia jų paslaugas Lietuvos Respublikos institucijoms.

16. Sąveikumo programos tinklų paslaugų teikimą Lietuvos Respublikos institucijoms reglamentuoja Elektroninio keitimosi duomenimis su Europos Sąjungos ir valstybių narių administracijomis taisyklės, patvirtintos Lietuvos Respublikos vidaus reikalų ministro 2004 m. vasario 24 d. įsakymu Nr. 1V-50 „Dėl Elektroninio keitimosi duomenimis su Europos Sąjungos ir valstybių narių administracijomis taisyklių patvirtinimo“.

17. SVDPT Lietuvos Respublikos institucijoms teikia šias paslaugas:

17.1. Duomenų perdavimo tarp Lietuvos Respublikos institucijų ir Europos Sąjungos institucijų ir organų bei jos valstybių narių institucijų, kurį sudaro:

17.1.1. saugus duomenų perdavimas SVDPT R srityje – saugioje pagrindinėje SVDPT srityje, skirta duomenų perdavimui tarp institucijų ir neturinčioje ryšių su viešaisiais elektroninių ryšių tinklais, bei SVDPT E srityje – apsaugotoje SVDPT srityje duomenų mainams tarp institucijų ir kitų viešojo administravimo subjektų, su kuriais sudarytos duomenų mainų sutartys;

17.1.2. sąveikos su Europos Sąjungos bei jos valstybių narių institucijų valdomais informaciniais ištekliais per TESTA ir kitus Sąveikumo programos tinklus valdymas;

17.1.3. prieigos prie institucijų valdomų valstybės informacinių išteklių teisių valdymas ir kitos saugumo valdymo priemonės;

17.1.4. SVDPT infrastruktūros teikimas informacinėms sistemoms ir registrams;

17.1.5. kitos susijusios priemonės.

17.2. Valstybės informacinių išteklių apsaugą nuo grėsmių iš viešųjų tinklų, kurią sudaro:

17.2.1. saugus duomenų perdavimas SVDPT D srityje – apsaugotoje SVDPT srityje duomenų mainams tarp institucijų, fizinių ir juridinių asmenų, kurioje talpinami valstybės informaciniai ištekliai, pasiekiami iš viešųjų elektroninių ryšių tinklų;

17.2.2. kolektyvinės apsaugos nuo grėsmių iš viešųjų tinklų apsaugos priemonės;

17.2.3. SVDPT D srities infrastruktūros teikimas valstybės informacinių išteklių tvarkytojams;

17.2.4. sąsajos su viešaisiais elektroninių ryšių tinklais valdymas;

17.2.5. kitos susijusios priemonės.

17.3. SVDPT informacinių ryšių technologijų infrastruktūros teikimą Lietuvos Respublikos institucijoms, kurį sudaro:

17.3.1. saugus duomenų perdavimas tarp institucijos padalinių;

17.3.2. prieigos prie institucijos valstybės informacinių išteklių teisių valdymas ir kitos saugumo valdymo priemonės;

17.3.3. SVDPT informacinių ryšių technologijų infrastruktūros teikimas institucijos informacinėms sistemoms;

17.3.4. saugi institucijos vietinių kompiuterinių tinklų infrastruktūra;

17.3.5. sąsajos su viešaisiais elektroninių ryšių tinklais valdymas;

17.3.6. kitos susijusios priemonės.

17.4. Elektroninio bendradarbiavimo tarp institucijų priemonės, kurias sudaro:

17.4.1. tarpinstitucinis telefono ryšys;

17.4.2. tarpinstitucinės vaizdo konferencijos;

17.4.3. tarpinstitucinis uždaras elektroninis paštas;

17.4.4. kitos susijusios priemonės.

_____