VIEŠŲJŲ PIRKIMŲ TARNYBOS
DIREKTORIUS

ĮSAKYMAS
DĖL VIEŠŲJŲ PIRKIMŲ TARNYBOS INFORMACINIŲ SISTEMŲ SAUGOS DOKUMENTŲ PATVIRTINIMO

2018 m. lapkričio 26 d. Nr. 1S-158
Vilnius

Vadovaudamasi Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ 7 ir 8 punktais ir Viešųjų pirkimų tarnybos nuostatų, patvirtintų Lietuvos Respublikos Vyriausybės 2017 m. spalio 31 d. nutarimu Nr. 889 „Dėl Lietuvos Respublikos Vyriausybės 2011 m. gruodžio 21 d. nutarimo Nr. 1517 „Dėl Viešųjų pirkimų tarnybos nuostatų patvirtinimo“ pakeitimo“, 18.1 ir 18.6 punktais:

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

1.1. Viešųjų pirkimų tarnybos informacinių sistemų duomenų saugos nuostatus;

1.2. Viešųjų pirkimų tarnybos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisykles;

1.3. Viešųjų pirkimų tarnybos informacinių sistemų veiklos tęstinumo valdymo planą;

ried1.4. Viešųjų pirkimų tarnybos informacinių sistemų naudotojų administravimo taisykles.

2. S k i r i u Viešųjų pirkimų tarnybos Elektroninių pirkimų skyriaus vedėją Vytautą Kovaliūną Viešųjų pirkimų tarnybos informacinių sistemų saugos įgaliotiniu ir kibernetinio saugumo vadovu.

3. P a v e d u:

3.1. Viešųjų pirkimų tarnybos Elektroninių pirkimų skyriaus vedėjui Vytautui Kovaliūnui ne vėliau kaip per 5 darbo dienas pateikti: Registrų ir valstybės informacinių sistemų registrui – patvirtintų duomenų saugos nuostatų kopiją ir patvirtintą teisės akto, kuriuo patvirtinti informacinės sistemos nuostatai, kopiją; Valstybės informacinių išteklių atitikties elektroninės informacijos saugos reikalavimams stebėsenos sistemai – saugos politiką įgyvendinančių dokumentų kopijas.

3.2. Tarnybos Administravimo skyriaus vyriausiajai specialistei Linai Bareikytei su šiuo įsakymu per elektroninę dokumentų valdymo sistemą supažindinti Elektroninių pirkimų skyriaus darbuotojus.

4. P r i p a ž į s t u netekusiu galios Viešųjų pirkimų tarnybos direktoriaus 2018 m. sausio 22 d. įsakymą Nr. 1S-12 „Dėl Viešųjų pirkimų tarnybos informacinių sistemų saugos dokumentų patvirtinimo“.

Direktorė Diana Vilytė

PATVIRTINTA
Viešųjų pirkimų tarnybos
direktoriaus 2018 m. lapkričio 26 d.
įsakymu Nr. 1S-158

VIEŠŲJŲ PIRKIMŲ TARNYBOS INFORMACINIŲ SISTEMŲ DUOMENŲ SAUGOS NUOSTATAI

I. BENDROSIOS NUOSTATOS

1. Viešųjų pirkimų tarnybos informacinių sistemų duomenų saugos nuostatų (toliau – Saugos nuostatai) tikslas sudaryti sąlygas saugiai automatizuotu būdu tvarkyti elektroninę informaciją Viešųjų pirkimų tarnybos (toliau – Tarnybos) informacinėse sistemose (toliau – TIS) užtikrinant TIS elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą.

2. Šiuose Saugos nuostatuose vartojamos sąvokos:

2.1. Tarnybos informacinės sistemos (TIS) – Centrinė viešųjų pirkimų informacinė sistema (toliau – CVP IS), Vidaus administravimo informacinė sistema ir Viešųjų pirkimų rizikos valdymo informacinė sistema (toliau – VPRV IS).

2.2. TIS ištekliai - informacijos, kurią valdo Tarnyba, atlikdama teisės aktų nustatytas funkcijas, apdorojamos informacinių technologijų priemonėmis, ir ją apdorojančių informacinių technologijų priemonių visuma.

2.3. TIS vidaus administratorius – Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atliekantis TIS priežiūrą.

2.4. TIS išorės administratorius – asmuo, pagal Tarnybos pasirašytą paslaugų teikimo sutartį, atliekantis TIS priežiūrą.

2.5. TIS vidaus naudotojas – Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis TIS ištekliais numatytoms darbo ar valstybės tarnybos funkcijoms atlikti.

2.6. TIS išorės naudotojas (pagal sutartį) – asmuo, kuris nėra Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, bet pagal Tarnybos pasirašytą duomenų teikimo sutartį, turintis teisę naudotis TIS ištekliais duomenų teikimo sutartyje ar teisės aktuose numatytoms funkcijoms atlikti.

2.7. TIS išorės naudotojas (pagal įstatymą) – asmuo, kuris nėra Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, tačiau vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymu, Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymu, Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymu, Lietuvos Respublikos koncesijų įstatymu turi teisę naudotis TIS ištekliais įstatyme numatytoms funkcijoms atlikti.

2.8. **Saugos dokumentai** – TIS saugos nuostatai ir TIS saugos politiką įgyvendinantys dokumentai.

2.9. Kibernetinio saugumo vadovas - kompetentingas asmuo, atsakingas už kibernetinio saugumo organizavimą ir užtikrinimą.

2.10. Kitos Saugos nuostatuose vartojamos sąvokos atitinka Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme ir kituose teisės aktuose, kuriais vadovaujamasi tvarkant TIS ir jose saugomus duomenis, bei Lietuvos standartuose LST ISO/IEC 27002:2017 ir LST ISO/IEC 27001:2017 vartojamas sąvokas.

3. TIS elektroninės informacijos saugumo tikslai:

3.1. sudaryti sąlygas TIS vidaus naudotojams, TIS išorės naudotojams (pagal sutartį), TIS išorės naudotojams (pagal įstatymą) saugiai pasiekti ir tvarkyti TIS elektroninę informaciją;

3.2. užtikrinti, kad TIS elektroninė informacija, būtų patikima ir apsaugota nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, kokio nors kitokio neteisėto jos tvarkymo.

4. TIS elektroninės informacijos, saugumo užtikrinimo prioritetinės kryptys:

4.1. TIS elektroninės informacijos, konfidencialumo, vientisumo, prieinamumo užtikrinimas;

4.2. TIS veiklos tęstinumo užtikrinimas;

4.3 TIS vidaus naudotojų, TIS išorės naudotojų (pagal sutartį) ir TIS išorės naudotojų (pagal įstatymą) mokymas.

5. TIS valdytoja ir tvarkytoja yra Tarnyba, kurios buveinės adresas Kareivių g. 1, LT-08221 Vilnius.

6. Tarnyba, kaip TIS valdytoja atlieka šias funkcijas:

6.1. valdo TIS;

6.2. peržiūri ir teikia tikslinti TIS tikslus, inicijuoja Saugos nuostatų keitimą;

6.3. rengia teisės aktus, susijusius su TIS tvarkymu;

6.4. rengia ir įgyvendina TIS plėtros projektus;

6.5. planuoja TIS pokyčių valdymą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčių tipą (administracinis, organizacinis ar techninis), įtakos vertinimą ir pokyčių prioritetų nustatymo procesus;

6.6. analizuoja teisines, technines, technologines, metodologines ir organizacines TIS tvarkymo problemas ir pagal savo kompetenciją priima sprendimus, reikalingus užtikrinant TIS tvarkymą;

6.7. vykdo kitas teisės aktų nustatytas funkcijas.

7. Tarnyba, kaip TIS tvarkytoja atlieka šias funkcijas:

7.1. užtikrina TIS techninės ir programinės įrangos įdiegimą, funkcionavimą ir atnaujinimą;

7.2. užtikrina TIS elektroninės informacijos saugą;

7.3. vykdo kitas teisės aktų nustatytas funkcijas.

8. TIS saugos įgaliotinis, įgyvendindamas TIS elektroninės informacijos saugą, atlieka šias funkcijas:

8.1. teikia Tarnybos vadovui pasiūlymus dėl:

8.1.1. TIS vidaus administratoriaus(-ių) paskyrimo ir reikalavimų administratoriui (-iams) nustatymo;

8.1.2. Saugos dokumentų priėmimo, keitimo ar panaikinimo;

8.1.3. TIS saugos reikalavimų atitikties vertinimo atlikimo;

8.2. koordinuoja TIS elektroninės informacijos saugos incidentų, įvykusių TIS, tyrimą ir bendradarbiauja su kompetentingomis institucijomis, tiriančiomis elektroninių ryšių tinklų informacijos saugumo incidentus, neteisėtas veikas, susijusias su TIS elektroninės informacijos saugos incidentais;

8.3. teikia TIS vidaus administratoriui(-iams) privalomus vykdyti nurodymus ir pavedimus;

8.4. organizuoja rizikos įvertinimą;

8.5. periodiškai organizuoja TIS vidaus naudotojų mokymą TIS elektroninės informacijos saugos klausimais, įvairiais būdais informuoja juos apie informacijos saugos problematiką (priminimai elektroniniu paštu, teminių seminarų rengimas, atmintinės naujiems vidaus naudotojams ar išorės naudotojams (pagal įstatymą) ir panašiai);

8.6. atlieka kitas Tarnybos vadovo pavestas ir 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“, jam priskirtas funkcijas;

8.7. TIS saugos įgaliotinis negali atlikti administratoriaus funkcijų.

9. TIS vidaus administratorius, atlieka šias funkcijas:

9.1. vertina TIS vidaus naudotojų pasirengimą dirbti su TIS;

9.2. valdo TIS naudotojų teises (suteikia, panaikina, redaguoja, keičia ir pan.);

9.3. atlieka saugumo reikalavimų atitikties nustatymą ir stebėseną;

9.4. reaguoja į TIS elektroninės informacijos saugos incidentus;

9.5. vykdo visus TIS saugos įgaliotinio nurodymus ir pavedimus, susijusius su informacinės sistemos saugos užtikrinimu;

9.6. teikia TIS saugos įgaliotiniui informaciją apie saugą užtikrinančių komponentų būklę;

9.7. atlieka TIS vidaus naudotojams, TIS išorės naudotojams (pagal sutartį) ir TIS išorės naudotojams (pagal įstatymą) suteiktų teisių ir priskirtų funkcijų atitikties vertinimą;

9.8. kontroliuoja išorės administratorių darbą;

9.9. rengia ir tikrina (peržiūri) TIS sudarančių komponentų sąranką;

9.10. nustato TIS pažeidžiamas vietas;

9.11. informuoja TIS saugos įgaliotinį apie Saugos dokumentuose nustatytų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones.

10. TIS išorės administratorius, pagal paskirtą kompetenciją, atlieka šias funkcijas:

10.1. rengia ir tikrina (peržiūri) TIS sudarančių komponentų sąranką;

10.2. nustato TIS pažeidžiamas vietas;

10.3. informuoja TIS saugos įgaliotinį apie Saugos dokumentuose nustatytų reikalavimų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones.

11. Kibernetinio saugumo vadovas:

11.1. priima sprendimus dėl laikino slaptažodžio perdavimo atviru tekstu, tačiau atskirai nuo prisijungimo vardo, jeigu TIS naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio ar nėra techninių galimybių TIS naudotojui perduoti slaptažodį saugiu elektroninių ryšių tinklu;

11.2. periodiškai peržiūri patvirtintų asmenų, kuriems suteiktos TIS administratoriaus teisės prisijungti prie TIS, sąrašus;

11.3. reaguoja į TIS kibernetinio saugumo incidentus;

11.4. analizuoja auditų duomenis;

11.5. priima sprendimus dėl naudojimosi belaidžiu tinklu ir mobiliaisiais įrenginiais, skirtais prisijungti prie TIS.

12. Teisės aktai, kuriais vadovaujamasi tvarkant TIS elektroninę informaciją ir šiose sistemose tvarkomus duomenis ir užtikrinant jų saugumą:

12.1. Lietuvos Respublikos viešųjų pirkimų įstatymas;

12.2. **Lietuvos Respublikos energijos išteklių rinkos įstatymas;**

12.3. **Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje** įstatymas;

12.4. Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymas;

12.5. Lietuvos Respublikos koncesijų įstatymas;

12.6. Lietuvos Respublikos kibernetinio saugumo įstatymas;

12.7. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

12.8. Valstybės informacinių išteklių valdymo įstatymas;

12.9. Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2013 m. vasario 27 d. nutarimu Nr. 180 „Dėl Valstybės informacinių sistemų steigimo, kūrimo, modernizavimo ir likvidavimo tvarkos aprašo patvirtinimo“;

12.10. Bendrųjų elektroninės informacijos saugos reikalavimų aprašas ir Saugos dokumentų turinio gairių aprašas, patvirtinti 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“;

12.11. Lietuvos Respublikos standartuose LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo priemonių praktikos nuostatai“, LST ISO/IEC 27001:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo valdymo sistemos. Reikalavimai“;

12.12. Centrinės viešųjų pirkimų informacinės sistemos nuostatai, patvirtinti Viešųjų pirkimų tarnybos direktoriaus 2017 m. birželio 6 d. įsakymu Nr. 1S-79 „Dėl Viešųjų pirkimų tarnybos direktoriaus 2010 m. spalio 11 d. įsakymo Nr. 1S-146 „Dėl Centrinės viešųjų pirkimų informacinės sistemos nuostatų patvirtinimo“ pakeitimo“;

12.13. Viešųjų pirkimų rizikos informacinės sistemos nuostatai, patvirtinti Viešųjų pirkimų tarnybos direktoriaus 2013 m. rugsėjo 16 d. įsakymu Nr. 1S-173 „Dėl Viešųjų pirkimų rizikos valdymo informacinės sistemos nuostatų patvirtinimo“;

12.14. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas, patvirtintas 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“ (toliau - Organizacinių ir techninių reikalavimų aprašas);

12.15. kiti teisės aktai, reglamentuojantys duomenų tvarkymo teisėtumą, duomenų saugos valdymą bei informacinių sistemų valdytojų ir tvarkytojų veiklą.

II. TIS ELEKTRONINĖS INFORMACIJOS SAUGOS VALDYMAS

13. Vadovaujantis Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ (toliau – Informacijos svarbos įvertinimo gairių aprašas) 8 punktu CVP IS tvarkoma informacija priskiriama svarbios informacijos kategorijai. Priskyrimo šiai elektroninės informacijos svarbos kategorijai kriterijai: CVP IS informacijos praradimas gali pažeisti daugiau nei 5 procentų, bet ne daugiau nei pusės valstybės gyventojų teises ir teisėtus

interesus, lemti, kad nebus atliekama (-os) kuri nors (kurios nors) gyvybiškai svarbi (-ios) funkcija (-os) daugiau nei vienam ministrui pavestose valdymo srityse ir vienai ar kelioms institucijoms padaryti finansinių nuostolių, didesnių nei 300 000 eurų, bet ne didesnių nei 3 000 000 eurų.

14. Vadovaujantis Informacijos svarbos įvertinimo gairių aprašo 9 punktu VPRV IS tvarkoma informacija priskiriama vidutinės svarbos informacijos kategorijai. Priskyrimo šiai elektroninės informacijos svarbos kategorijai kriterijai: VPRV IS praradimas gali pažeisti daugiau nei 1 procento, bet ne daugiau nei 5 procentų valstybės gyventojų teises ir teisėtus interesus, lemti, kad nebus atliekama (-os) kuri nors (kurios nors) gyvybiškai svarbi (-ios) funkcija (-os) vienam ministrui pavestoje valdymo srityje ir vienai ar kelioms institucijoms padaryti finansinių nuostolių, didesnių nei 30 000 eurų, bet ne didesnių nei 300 000 eurų.

15. Vadovaujantis Informacijos svarbos įvertinimo gairių aprašo 10 punktu Tarnybos vidaus administravimo informacinėje sistemoje tvarkoma informacija priskiriama mažiausios svarbos informacijos kategorijai.

16. Vadovaujantis Informacijos svarbos įvertinimo gairių aprašo 12.2 papunkčiu CVP IS, priskiriama antrajai informacinių sistemų kategorijai.

17. Vadovaujantis Informacijos svarbos įvertinimo gairių aprašo 12.3 papunkčiu VPRV IS, priskiriama trečiajai informacinių sistemų kategorijai.

18. Vadovaujantis Informacijos svarbos įvertinimo gairių aprašo 12.4 papunkčiu Tarnybos vidaus administravimo informacinė sistema, priskiriama ketvirtajai informacinių sistemų kategorijai.

19. TIS saugos įgaliotinis, atsižvelgdamas į Vidaus reikalų ministerijos išleistą metodinę priemonę „Rizikos analizės vadovas“, Lietuvos standartą LST ISO/IEC 27005:2011 „Informacijos technologija. Saugumo technika. Informacijos saugumo rizikos valdymas“, kasmet organizuoja Informacinių sistemų rizikos įvertinimą. Prireikus TIS saugos įgaliotinis gali organizuoti neeilinį Informacinių sistemų rizikos įvertinimą. Tarnybos vadovo rašytiniu pavedimu Informacinių sistemų rizikos įvertinimą gali atlikti pats TIS saugos įgaliotinis.

20. TIS rizikos įvertinimas išdėstomas rizikos įvertinimo ataskaitoje, kartu su pagrindiniu informacinės sistemos rizikos vertinimu organizuojamas ir atliekamas grėsmių ir pažeidžiamumų, galinčių turėti įtakos informacinės sistemos kibernetiniam saugumui vertinimas. Rizikos įvertinimo ataskaita rengiama atsižvelgiant į rizikos veiksnius, galinčius turėti įtakos informacijos saugai. Svarbiausi rizikos veiksniai yra šie:

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

20.2. subjektyvūs tyčiniai (nesankcionuotas naudojimasis TIS elektroninei informacijai gauti, duomenų pakeitimas ar sunaikinimas, informacinių technologijų duomenų perdavimo tinklais sutrikdymai, saugumo pažeidimai, duomenų vagystės ir kita);

20.3. nenugalima jėga (*force majeure*).

21. Rizikos veiksniai vertinami pagal TIS elektroninės informacijos kategorijas, nustatant jų įtakos TIS esančios elektroninės informacijos saugai laipsnius:

21.1. Ž – žemas. Duomenų pažeidimo poveikio laipsnis nėra didelis, padariniai nebus pavojingi – TIS elektroninė informacija pasiųsta kitam adresatui, įvesti netikslūs duomenys, prarasta TIS elektroninė informacija po paskutinio kopijavimo;

21.2. V – vidutinis. Duomenų pažeidimo poveikio laipsnis gali būti didelis, padariniai rimti – duomenys iš dalies prarasti, duomenų bazių įrašai suklastoti, neveikia kompiuterinės programos ir operacinė sistema;

21.3. A – aukštas. Duomenų pažeidimo poveikio laipsnis labai didelis, padariniai ypatingai rimti – duomenys visiškai prarasti, prarasti ne tik duomenys iš duomenų bazių, bet ir atsarginės kopijos, neveikia visa informacinė sistema.

22. Rizikos vertinimo metu atliekamų darbų apimtis:

22.1. TIS išteklių inventorizacija;

22.2. įtakos TIS veiklai vertinimas;

22.3. grėsmės ir pažeidžiamumų analizė;

22.4. liekamosios rizikos vertinimas.

23. Atsižvelgdamas į rizikos įvertinimo ataskaitą, Tarnybos vadovas prireikus tvirtina Rizikos įvertinimo ir rizikos valdymo priemonių planą, kuriame, be kita ko, numatomas techninių, administracinių ir kitų išteklių poreikis rizikos valdymo priemonėms įgyvendinti.

24. Pagrindiniai TIS elektroninės informacijos saugos priemonių parinkimo principai yra šie:

24.1. liekamoji rizika turi būti mažinama, atsižvelgiant į rizikos valdymo priemonių planą;

24.2. informacijos saugos priemonių diegimo kaina adekvati saugomos informacijos vertei;

24.3. turi būti įdiegtos kibernetinės saugos pažeidžiamumų stebėsenos ir detektavimo priemonės;

24.4. pirmenybė teikiama toms priemonėms, kurių įdiegimas duoda didžiausią efektą ir reikalauja mažiausiai sąnaudų;

24.5. pirmenybė teikiama toms priemonėms, kurios skirtos išsaugoti elektroninę informaciją, kurios praradimas turėtų didžiausią įtaką Informacinių sistemų ir Tarnybos veiklai;

24.6. TIS turi turėti įvestos TIS elektroninės informacijos tikslumo, užbaigtumo ir patikimumo tikrinimo priemonių.

25. Siekiant užtikrinti šiuose nuostatuose ir kituose Saugos dokumentuose išdėstytų nuostatų įgyvendinimo kontrolę, ne rečiau kaip kartą per metus organizuojamas informacinių technologijų saugos atitikties vertinimas, kurio metu:

25.1. įvertinama šių nuostatų ir kitų TIS saugą reglamentuojančių teisės aktų ir realios informacijos saugos atitiktis;

25.2. inventorizuojama TIS techninė ir programinė įranga;

25.3. tikrinama TIS tarnybinėse stotyse įdiegta programinė įranga ir jos sąranka;

25.4. patikrinama ne mažiau kaip 10% atsitiktinai pasirinktų TIS naudotojų kompiuterių;

25.5. patikrinama (įvertinama) TIS elektroninę informaciją tvarkantiems TIS vidaus naudotojams, TIS išorės naudotojams (pagal sutartį), TIS vidaus administratoriams ir TIS išorės administratoriams suteiktų teisių atitiktis vykdomoms funkcijoms;

25.6. įvertinamas pasirengimas užtikrinti TIS veiklos tęstinumą, įvykus saugos incidentui.

26. Atlikus šių nuostatų 25 punkte nurodytą vertinimą, rengiama informacinių technologijų saugos atitikties vertinimo ataskaita ir pastebėtų trūkumų šalinimo planas, kurį tvirtina, atsakingus vykdytojus paskiria ir įgyvendinimo terminus nustato Tarnybos vadovas.

27. Kibernetinių incidentų valdymas atliekamas vadovaujantis Nacionaliniu kibernetinių incidentų valdymo planu, patvirtintu Lietuvos Respublikos Vyriausybės 2016 m. sausio 25 d. nutarimu Nr. 87 „Dėl nacionalinio kibernetinių incidentų valdymo plano patvirtinimo“.

28. Rizikos įvertinimo ataskaitos, rizikos įvertinimo ir rizikos valdymo priemonių plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

29. Informacinių technologijų saugos atitikties vertinimo ataskaitos, pastebėtų trūkumų šalinimo plano kopijas informacinės sistemos valdytojas ne vėliau kaip per 5 darbo dienas nuo minėtų dokumentų priėmimo turi pateikti Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemai Valstybės informacinių išteklių atitikties elektroninės informacijos saugos (kibernetinio saugumo) reikalavimams stebėsenos sistemos nuostatų nustatyta tvarka.

30. Informacinės sistemos informacinių technologijų saugos atitikties Lietuvos standartui LST ISO/IEC 27002:2017 vertinimą atlieka nepriklausomi specialistai.

31. Informacinių sistemų informacinių technologijų saugos atitikties vertinimo metu gali būti atliekamas pažeidžiamumų testavimas imituojant kibernetines atakas bei vykdant kibernetinių incidentų imitavimo pratybas. Imituojant kibernetines atakas rekomenduojama vadovautis tarptautiniu mastu pripažintų organizacijų (pvz., EC-COUNCIL, ISACA, NIST ir kt.) rekomendacijomis ir gerąja praktika.

III. ORGANIZACINIAI IR TECHNINIAI REIKALAVIMAI

32. Informacinėse sistemose esanti TIS elektroninė informacija teikiama ir (ar) gaunama vadovaujantis Viešųjų pirkimų įstatymu, Energijos išteklių rinkos įstatymu, **Viešųjų pirkimų, atliekamų gynybos ir saugumo srityje** įstatymu, Pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymu, Koncesijų įstatymu arba TIS elektroninės informacijos arba duomenų teikimo sutartimis, kuriose turi būti nurodyta:

32.1. duomenų naudojimo sąlygos ir tikslai;

32.2. duomenų teikimo ir (ar) gavimo būdai ir terminai;

32.3. duomenų teikimo ir (ar) gavimo specifikacija ir kitos sąlygos.

33. TIS išorės administratoriai ir naudotojai (pagal sutartį) prie TIS jungiasi tik naudodamiesi techninėmis ir programinėmis priemonėmis, užtikrinančiomis saugų duomenų perdavimą kompiuterių tinklais.

34. TIS elektroninės informacijos saugai užtikrinti taikomos šios bendrosios programinės įrangos naudojimo nuostatos:

34.1. TIS tarnybinėse stotyse, TIS vidaus administratorių, TIS vidaus naudotojų kompiuteriuose gali būti naudojama tik legali programinė įranga, kuri turi licencijas, suteikiančias teisę ją naudoti. Jei tokių licencijų programinės įrangos gamintojai nenumato, turi būti pateikiamos nuorodos į šaltinius, vienareikšmiškai nurodančius, kad programinę įrangą galima naudoti nemokamai;

34.2. TIS tarnybinėse stotyse, TIS vidaus administratorių, TIS vidaus naudotojų kompiuteriuose naudojama antivirusinė programinė įranga privalo turėti automatinį atnaujinimą; Ilgiausias leistinas antivirusinės programinės įrangos neatnaujinimo laikas - ne ilgiau kaip 5 darbo dienos;

34.3. TIS tarnybinėse stotyse, TIS vidaus administratorių, TIS vidaus naudotojų kompiuteriuose programinės įrangos atnaujinimai ir pataisymai turi būti įdiegti ne vėliau kaip per 5 dienas nuo jų išleidimo.

35. TIS elektroninės informacijos, saugai užtikrinti TIS tarnybinėse stotyse taikomos šios programinės įrangos naudojimo nuostatos:

35.1. sisteminės ir taikomosios programinės įrangos sąranka parenkama tokiu būdu, kad būtų užtikrinamas didžiausias galimas saugumo lygis, stabdomi nereikalingi darbui procesai;

35.2. programinę įrangą kontroliuoja, jos pataisymus ir atnaujinimus diegia atitinkamos TIS vidaus administratorius arba TIS išorės administratorius, arba atitinkamų paslaugų teikėjas. Minėtus darbus paslaugų teikėjai gali atlikti tik suderinę arba dalyvaujant Tarnybos Elektroninių pirkimų skyriaus (toliau – EPS) darbuotojams.

36. TIS elektroninės informacijos saugai užtikrinti TIS vidaus administratorių ir TIS vidaus naudotojų kompiuteriuose taikomos šios programinės įrangos naudojimo nuostatos:

36.1. programinę įrangą kontroliuoja, jos pataisymus ir atnaujinimus diegia TIS vidaus administratoriai (EPS darbuotojai);

36.2. kompiuteriuose gali būti įdiegta tiktai tokia programinė įranga, kuri reikalinga darbuotojo pareigybės aprašyme numatytoms funkcijoms atlikti.

37. TIS elektroninės informacijos perdavimo tinklas turi būti atskirtas nuo viešųjų telekomunikacijų tinklų kompiuterių tinklo ugniasienėmis.

38. Kompiuterių tinklo ugniasienės turi būti sukonfigūruotos taip, kad būtų praleidžiamas tik toks TIS elektroninės informacijos srautas, kuris yra būtinas Tarnybos veiklai.

39. Už kompiuterių tinklo ugniasienių administravimą, priežiūrą, nustatymų atnaujinimą atsakingi TIS išorės administratoriai. Ugniasienės įvykių žurnalai (angl. *Logs*) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos.

40. Kompiuterių tinklo ugniasienių nustatymų aprašymai saugomi Tarnybos EPS. TIS saugos įgaliotinio iniciatyva, ne rečiau kaip kartą per metus turi būti peržiūrima kompiuterių tinklo ugniasienių nustatymai.

41. TIS vidaus ir išorės naudotojai privalo rūpintis TIS tvarkomų duomenų saugumu.

42. TIS vidaus ir išorės naudotojai, pastebėję TIS saugos dokumentų pažeidimus, nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugos užtikrinimo priemones, privalo nedelsdami pranešti apie tai administratoriui ir saugos įgaliotiniui.

43. Jeigu saugos įgaliotinis nebuvo informuotas apie Saugos nuostatų 43 punkte nurodytus pažeidimus, administratorius informuoja saugos įgaliotinį apie šiuos pažeidimus. Įtaręs neteisėtą veiką, pažeidžiančią ar neišvengiamai pažeisiančią TIS saugą (jos konfidencialumą, vientisumą ar prieinamumą), saugos įgaliotinis apie tai turi pranešti TIS valdytojo vadovui ir kompetentingoms institucijoms, tiriančioms elektroninių ryšių tinklų, informacijos saugumo incidentus, neteisėtas veikas, susijusias su elektroninės informacijos saugos incidentais.

44. Pagrindiniai reikalavimai TIS elektroninės informacijos atsarginių kopijų darymui ir atkūrimui yra tokie:

44.1. TIS elektroninės informacijos atsarginės kopijos daromos periodiškai, bet ne rečiau kaip vieną kartą per savaitę pagal TIS atsarginių TIS elektroninės informacijos kopijų valdymo tvarką;

44.2. TIS elektroninės informacijos atsarginių kopijų laikmenos saugomos rakinamoje nedegančioje spintoje, atskiroje nuo tarnybinių stočių patalpoje;

44.3. praradus TIS elektroninės informacijos dėl techninės įrangos gedimo, programinės įrangos klaidos ar kitaip pažeidus duomenų vientisumą, duomenys atkuriami iš vėliausiai įrašytų atsarginių duomenų kopijų;

44.4. duomenis atkuria atitinkamos TIS, kurios duomenys buvo prarasti ar kitaip sugadinti, vidaus administratorius ar išorės administratorius;

44.5. visi duomenų atkūrimo veiksmai turi būti protokoluojami, nurodant priežastį dėl kurios vykdomas duomenų atkūrimas, kokie duomenys buvo atkuriami, iš kokios atsarginių duomenų kopijos buvo vykdomas atkūrimas ir kas jį atliko;

44.6. atlikus duomenų atkūrimą, atitinkamos TIS vidaus administratorius ar TIS išorės administratorius atlieka šios informacinės sistemos funkcionalumo ir duomenų vientisumo bei parengtumo testavimą;

44.7. visi atitinkamos TIS, kurios duomenys buvo atkurti, TIS vidaus naudotojai, TIS išorės naudotojai (pagal sutartį) ir TIS išorės naudotojai (pagal įstatymą) informuojami apie įvykusį incidentą;

44.8. periodiškai, bet ne rečiau kaip vieną kartą metuose, TIS saugos įgaliotinio iniciatyva vykdomas bandomasis TIS duomenų atkūrimas iš TIS elektroninės informacijos atsarginių kopijų, kurio eiga ir rezultatai protokoluojami.

45. Užtikrinant saugų TIS elektroninės informacijos teikimą ir (ar) gavimą, prisijungimas nuotoliniu būdu suteikiamas:

45.1. TIS išorės administratoriams naudojant VPN (*angl. virtual private network* **)** arba RDP (*angl. remote desktop protocol*) ryšio protokolus;

45.2 TIS išorės naudotojams (pagal įstatymą) naudojant interneto ryšį ir koduojant siunčiamą informaciją;

45.3. TIS išorės naudotojams (pagal sutartį) pagal duomenų teikimo sutarčių sąlygose nustatytas specifikacijas ir sąlygas, naudojant VPN (*angl. Virtual Private Network*) ir FTPS (*angl. File Transfer Protocol Secure*) protokolą (susiejant su Informacinių sistemų naudotojo IP (*angl. Internet Protocol*) adresu).

46. TIS turi perspėti vidaus ir išorės administratorių, kai pagrindinėje TIS kompiuterinėje įrangoje sumažėja iki nustatytos pavojingos ribos laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterių tinklo sąsaja.

47. TIS interneto svetainėms turi būti taikomi Organizacinių ir techninių reikalavimų aprašo 2 priede nustatyti svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumo reikalavimai.

48. Leistinos kompiuterių naudojimo ribos:

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

48.2. nešiojamuosiuose kompiuteriuose ir kituose mobiliuosiuose įrenginiuose turi būti naudojamas įjungimo slaptažodis;

48.3. darbiniuose mobiliuose telefonuose turi būti įjungtas duomenų šifravimas;

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

49. Ne rečiau kaip kartą per mėnesį turi būti atliekama TIS vidaus ir išorės naudotojų veiksmų audito įrašų analizė.

50. Tarnybos svečiams skirtas belaidis tinklas turi būti visiškai (fiziškai ir logiškai) atskiras nuo Tarnybos TIS resursų. Šis tinklas turi būti apsaugotas slaptažodžiu, kuris pateikiamas atvykusiems svečiams. Slaptažodis turi būti keičiamas periodiškai (ne rečiau kaip 2 kartus į metus);

51. Tarnybos darbuotojams skirtas belaidis tinklas turi būti apsaugotas slaptažodžiu, bei susietas su Tarnybos naudotojų katalogu (angl. Active directory). Tik prie Active Directory prisijungusiems Tarnybos darbuotojams turi būti leidžiama prisijungti prie darbuotojų belaidžio tinklo.

52. TIS vidaus naudotojai turi žinoti, kad visa informacija, kuri sukuriama ar kitaip tvarkoma TIS yra Tarnybos nuosavybė.

53. Išskirtiniais atvejais, kai tai yra būtina Tarnybos veiklai užtikrinti, Vadovybės sprendimu privati TIS vidaus naudotojų informacija (sukurta, automatiškai sugeneruota ar kitaip tvarkoma informacija TIS bei TIS vidaus naudotojo atlikti veiksmai, įskaitant kompiuterių tinklo bei naršymo internete srautą ir trukmę, spausdinimo, telefonijos, elektroninio pašto ir kt. darbo funkcijoms atlikti patikėtų darbo priemonių naudojimo istorija), saugoma TIS, gali būti tvarkoma be TIS vidaus

naudotojo žinios. Tvarkant TIS vidaus naudotojo privačią informaciją užtikrinama, kad bus laikomasi asmens duomenų apsaugos principų teisės aktų nustatyta tvarka.

54. TIS vidaus naudotojai naudodamiesi elektroniniu paštu ir internetu privalo:

54.1. naudoti internetą ir elektroninį paštą tik darbo Tarnyboje reikalams;

54.2. užtikrinti, kad visų elektroninio pašto pranešimų bendras dydis elektroninio pašto dėžutėje neviršytų leistino dydžio (2 GB, išskyrus atvejus, kai yra suteiktas didesnis kiekis);

54.3. gavęs iš el. pašto įspėjimą apie išnaudotą elektroninio pašto dėžutės limitą, nedelsiant pašalinti nereikalingus pranešimus arba kitaip atlaisvinti vietą;

54.4. neatidaryti elektroninio pašto pranešimų, kuriuose yra failų su plėtiniais „*.com“, „*.exe“, „*.vbs“, „*.html“, nes šiuose failuose gali būti virusų. Nedelsiant pranešti Tarnybos EPS apie gautus tokius pranešimus;

54.5. šifruoti visą elektroniniu paštu siunčiamą konfidencialią informaciją, įskaitant priedus (pvz., pasinaudojant 7-zip. Programine įranga);

54.6. naudotojas, pastebėjęs Tarnybos sistemų veikimo sutrikimų, apie tai privalo nedelsdamas pranešti EPS;

54.7. siekiant užtikrinti duomenų saugumą, naudotojas privalo įdiegti visus mobilių nešiojamų įrenginių programinės įrangos atnaujinimus (galioja nešiojamiems kompiuteriams ir mob. telefonams, prijungtiems prie TIS resursų);

54.8. mobilių telefonų papildoma programinė įranga ar jos atnaujinimai turi būti diegiami tik darbo tikslais ir tik iš patikimų programinės įrangos šaltinių tokių kaip „iTunes Store“, „Android Play Store“;

54.9. nenaudoti kito Tarnybos naudotojo el. pašto adreso (taip pat nebandyti prisijungti kito TIS naudotojo vardu);

54.10. nekurti ir nepersiuntinėti grandininių el. laiškų, kuriuose skatinama persiųsti el. laišką savo kolegoms, pažystamiems ar pan.;

55. Naudojant internetą ir elektroninį paštą TIS vidaus naudotojams draudžiama (šių draudimų išimtys gali būti taikomos darbuotojams, kurių pagrindinėms darbo funkcijoms to reikalauja):

55.1. skelbti Tarnybos konfidencialią informaciją internete;

55.2. pažeisti asmenų teises, kurios saugomos prekės ženklų, patentų ar kitų intelektualios nuosavybės apsaugos teisės aktais (kopijuoti autorių teisių saugomą turinį ir pan.);

55.3. parsisiųsti arba platinti tiesiogiai su darbu nesusijusią grafinę, garso ir vaizdo medžiagą, žaidimus ir programinę įrangą, siųsti duomenis, kurie yra užkrėsti virusais, turi įvairius kitus žalingus programinius kodus, bylas, galinčias sutrikdyti kompiuterinių ar telekomunikacinių įrenginių bei programinės įrangos funkcionavimą ir saugumą;

55.4. savarankiškai keisti, taisyti Tarnybos informacinių technologijų techninę ir programinę įrangą;

55.5. atskleisti prisijungimo prie Tarnybos sistemų duomenis kitiems asmenims (įskaitant šeimos narius, jei dirbama namuose);

55.6. naudoti Tarnybos resursus teisės aktais draudžiamai veiklai atlikti (šmeižiančio, įžeidžiančio, grasinamojo ar trukdančio pobūdžio informacijai, kompiuterių virusams siųsti).

55.7. naudoti Tarnybos resursus kaupt ar platinti įžeidžiančio, pornografinio ar panašaus turinio informaciją;

55.8. bet kokia forma diskriminuoti ar priekabiauti naudojantis el. paštu, telefonu ar bet kokia kita forma;

55.9. naudoti elektroninį paštą ir interneto prieigą asmeniniams, komerciniams tikslams, siūlyti ne Tarnybos teikiamas paslaugas, naudojantis Tarnybos vardu;

55.10. naudoti įrangą neteisėtai prieigai prie Tarnybos sistemų ar jos duomenų saugumo tikrinimui, skenavimui, kompiuterinio tinklo srauto duomenų stebėjimui;

55.11. rinkti kompiuterių tinklu perduodamus duomenis ar jų fragmentus, analizuoti jų pobūdį, kiekį, nebent tai būtina atliekant teisėtas veiklos funkcijas;

55.12. bandyti apeiti Tarnybos naudotojo prieigos prie Tarnybos sistemų tapatybės nustatymo mechanizmus;

55.13. perduoti Tarnybai priklausančią IT techninę ir programinę įrangą (duomenis) tretiesiems asmenims, jei toks perdavimas nėra susijęs su darbinių funkcijų vykdymu.

IV. REIKALAVIMAI PERSONALUI

56. TIS saugos įgaliotinis privalo išmanyti TIS elektroninės informacijos saugos užtikrinimo principus, savo darbe vadovautis teisės aktais, standartais ir kitais dokumentais, reglamentuojančiais saugų TIS elektroninės informacijos tvarkymą, atitikti pareigybės aprašyme numatytą specialųjį išsilavinimo reikalavimą, tobulinti kvalifikaciją TIS elektroninės informacijos saugos srityje, gebėti prižiūrėti, kaip įgyvendinami Saugos dokumentai, turėti darbo su kompiuterių technine bei programine įranga patirties.

57. TIS vidaus administratoriai privalo gerai išmanyti kompiuterių tinklų ir tarnybinių stočių technines ir sistemines programines priemones, turėti patirties ir mokėti administruoti jas bei jų naudotojus, gerai žinoti kompiuterių tinklų ir tarnybinių stočių saugumo užtikrinimo principus ir mokėti juos taikyti, užtikrinant patikimą duomenų saugą bei Saugos dokumentų įgyvendinamą.

58. TIS išorės administratoriai privalo gerai išmanyti Tarnybos vidinių ir išorinių kompiuterių tinklų ir tarnybinių stočių technines ir sistemines programines priemones, turėti patirties ir mokėti administruoti jas bei jų naudotojus, gerai žinoti kompiuterių tinklų ir tarnybinių stočių saugumo užtikrinimo principus ir mokėti juos taikyti, užtikrinant patikimą duomenų saugą bei Saugos dokumentų įgyvendinamą.

59. TIS vidaus naudotojai privalo turėti pagrindinius darbo su kompiuteriais įgūdžius.

60. TIS vidaus naudotojai privalo susipažinti su tarnybinėms funkcijoms atlikti naudojamų Informacinių sistemų nuostatais, naudotojų instrukcijomis (vadovais), Saugos dokumentais ir laikytis jų reikalavimų.

61. TIS išorės naudotojai turi turėti pagrindinius darbo kompiuteriu įgūdžius, mokėti tvarkyti TIS elektroninę informaciją, TIS nuostatų nustatyta tvarka, būti susipažinę su Saugos nuostatais bei teisės aktais, reglamentuojančiais saugų elektroninės informacijos tvarkymą.

62. TIS vidaus naudotojai, TIS išorės naudotojai (pagal sutartį) ir TIS išorės naudotojai (pagal įstatymą) pastebėję TIS saugumo pažeidimus, neleistinos arba nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugą užtikrinančias priemones, privalo apie tai nedelsdami pranešti atitinkamos TIS elektroninės informacijos teikimo sutartyje nurodytam asmeniui ar TIS vidaus administratoriui, o pastarasis nedelsdamas informuoti TIS saugos įgaliotinį.

63. Už TIS vidaus administratorių, TIS saugos įgaliotinio, TIS kibernetinio saugumo vadovo, TIS vidaus naudotojų mokymų informacinių technologijų bei TIS elektroninės informacijos saugos srityse organizavimą atsakingas Tarnybos EPS. TIS naudotojų mokymai elektroninės informacijos saugos temomis vykdomi pagal poreikį, bet ne rečiau kaip kartą per dvejus metus.

V. INFORMACINĖS SISTEMOS NAUDOTOJŲ SUPAŽINDINIMO SU SAUGOS DOKUMENTAIS PRINCIPAI

64. Tvarkyti TIS esančią elektroninę informaciją gali tik TIS vidaus naudotojai ir TIS išorės naudotojai (pagal įstatymą) susipažinę su Saugos dokumentais ir pasirašytinai ar kitokiu būdu įsipareigoję laikytis jų reikalavimų.

65. TIS vidaus naudotojus su Saugos dokumentais ir atsakomybe už juose numatytų reikalavimų nesilaikymą pasirašytinai supažindina TIS saugos įgaliotinis. Turi būti užtikrintas susipažinimo įrodomumas.

66. TIS išorės naudotojai (pagal įstatymą) su Saugos dokumentais, paskelbtais Centrinėje viešųjų pirkimų informacinėje sistemoje, privalo susipažinti registruodamiesi, o patvirtindami registraciją įsipareigoja vadovautis šių dokumentų reikalavimais.

67. Pakartotinai su Saugos dokumentais TIS naudotojai supažindinami jiems pasikeitus.

68. Saugos dokumentai bei teisės aktai ir kita su duomenų sauga susijusi TIS elektroninė informacija patalpinama Tarnybos intraneto svetainėje, skyriuje „Duomenų sauga“.

69. TIS saugos įgaliotinis, TIS vidaus administratoriai, TIS išorės administratoriai, TIS vidaus naudotojai, TIS išorės naudotojai (pagal įstatymą), TIS išorės naudotojai (pagal sutartį), pažeidę Saugos dokumentų reikalavimus, atsako Lietuvos Respublikos teisės aktų nustatyta tvarka.

70. TIS naudotojai privalo saugoti duomenų ir informacijos paslaptį. Įsipareigojimas saugoti paslaptį galioja ir nutraukus su TIS elektroninės informacijos tvarkymu susijusią veiklą.

VI. BAIGIAMOSIOS NUOSTATOS

71. Saugos nuostatai iš esmės peržiūrimi ir prireikus keičiami ne rečiau kaip kartą per metus.

_____

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018 m. rugsėjo 25 d. raštu Nr. (4.2)6K-599

PATVIRTINTA
Viešųjų pirkimų tarnybos
direktoriaus 2018 m. lapkričio 26 d.
įsakymu Nr. 1S-158

VIEŠŲJŲ PIRKIMŲ TARNYBOS INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Viešųjų pirkimų tarnybos informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Taisyklės) tikslas – nustatyti tvarką, kuria vadovaujantis būtų saugiai tvarkoma Viešųjų pirkimų tarnybos (toliau – Tarnyba) Centrinėje viešųjų pirkimų informacinėje sistemoje (toliau – CVP IS), Tarnybos Vidaus administravimo informacinėje sistemoje (VA IS) ir Viešųjų pirkimų rizikos valdymo informacinėje sistemoje (toliau – VPRV IS) saugoma bei apdorojama informacija.

2. Taisyklės parengtos vadovaujantis šiais teisės aktais:

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

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

2.3. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V–832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

2.4. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas, patvirtintas 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“;

2.5. kitais teisės aktais, reglamentuojančiais saugų elektroninių duomenų tvarkymą.

3. Taisyklėse vartojamos sąvokos:

3.1. **Tarnybos informacinės sistemos (TIS)** – CVP IS, VA IS ir VPRV IS.

3.2. TIS išorės naudotojas (pagal įstatymą) – asmuo, kuris nėra Tarnybos darbuotojas, tačiau, vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymu (toliau – Įstatymas), Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymu (toliau – Gynybos įstatymas), Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymu, Lietuvos Respublikos koncesijų įstatymu, turi teisę naudotis TIS ištekliais Įstatyme bei Gynybos įstatyme numatytoms funkcijoms atlikti.

3.3. TIS išorės naudotojas (pagal sutartį) – asmuo, kuris nėra Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, bet pagal Tarnybos pasirašytą duomenų

teikimo sutartį, turintis teisę naudotis TIS ištekliais duomenų teikimo sutartyje ar teisės aktuose numatytoms funkcijoms atlikti.

3.4. TIS išorės administratorius – asmuo, pagal Tarnybos pasirašytą paslaugų teikimo sutartį, atliekantis TIS priežiūrą.

3.5. TIS vidaus administratorius – Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atliekantis TIS priežiūrą.

3.6. TIS vidaus naudotojas – Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis TIS ištekliais numatytoms darbo ar valstybės tarnybos funkcijoms atlikti.

3.7. Viešasis pirkimas – pirkimas, reglamentuotas Lietuvos Respublikos viešųjų pirkimų įstatymo ar Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymo ar Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymo ar Lietuvos Respublikos koncesijų įstatymo.

3.8. TIS valdytojas – Tarnyba.

4. Kitos taisyklėse vartojamos sąvokos atitinka Taisyklių 2 punkte nurodytuose teisės aktuose nustatytas sąvokas.

5. Vadovautis Taisyklėmis privalo visi TIS vidaus ir išorės naudotojai, TIS vidaus ir išorės administratoriai, TIS saugos įgaliotinis.

6. Už Taisyklių įgyvendinimą ir jų laikymosi kontrolę atsakingas TIS saugos įgaliotinis.

7. CVP IS saugoma bei apdorojama informacija apie viešuosius pirkimus priskiriama svarbiai elektroninės informacijos kategorijai, ją sudaro:

7.1. viešųjų pirkimų skelbimai;

7.2. viešųjų pirkimų ataskaitos;

7.3. viešųjų pirkimų sutartys;

7.4. viešųjų pirkimų dokumentai (vertinimai, tikrinimai, sutikimai, protokolai);

7.5. informacija apie viešųjų pirkimų procesą.

8. Už CVP IS saugomos TIS elektroninės informacijos tvarkymą atsakingi:

8.1. Tarnybos Prevencijos ir skelbimų skyrius, statistikos ir ataskaitų skyrius(7.1 ir 7.2 punktuose nurodyti duomenys);

8.2. Tarnybos Prevencijos ir pirkimo sutarčių priežiūros, Priežiūros skyrius (7.4 ir 7.5 punktuose nurodyti duomenys);

8.3. registruoti CVP IS išorės naudotojai (pagal įstatymą) (informacijos apie vykdomus ar įvykdytus viešuosius pirkimus teikimas ir tvarkymas CVP IS).

9. VPRV IS saugoma bei tvarkoma informacija priskiriama žinybinės svarbos elektroninės informacijos kategorijai, ją sudaro:

9.1. rizikos apskaičiavimui naudojami duomenys;

9.2. naudojamų kintamųjų ir rizikos rodiklių apskaičiavimui naudojami duomenys;

9.3. informacijos operatyviniam vertinimui duomenys;

9.4. rizikos valdymo duomenys;

9.5. profilių duomenys;

9.6. kintamųjų ir rizikų parametrų duomenys;

9.7. juodųjų ir baltųjų sąrašų duomenys;

9.8. rizikos valdymo efektyvumo rodiklių duomenys;

9.9. VPRV IS naudotojų duomenys.

10. Už VPRV IS elektroninės informacijos tvarkymą atsakingi:

10.1. VPRV IS vidaus naudotojai (9.1, 9.2, 9.3, 9.4, 9.5 punktuose nurodyti duomenys);

10.2. Tarnybos Rizikų valdymo skyriaus vedėjas (9.6, 9.7, 9.8 ir 9.9 punktuose nurodyti duomenys).

11. VA IS saugoma bei apdorojama informacija, priskiriama žinybinės svarbos elektroninės informacijos kategorijai, ją sudaro:

11.1. raštvedybos duomenys;
11.2. Tarnybos vidaus dokumentai;
11.3. VA IS naudotojų duomenys.
12. Už VA IS saugomos ir tvarkomos elektroninės informacijos tvarkymą atsakingi:
12.1. Tarnybos Administravimo skyrius (11.1 ir 11.2 punktuose nurodyti duomenys);
12.2. Tarnybos Elektroninių pirkimų skyrius (11.3 punkto duomenys).

II. TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

13. Saugiam TIS elektroninės informacijos tvarkymui užtikrinti naudojamos kompiuterinės, sisteminės ir taikomosios programinės įrangos, fizinės, techninės ir organizacinės duomenų saugos priemonės.

14. TIS techninės įrangos saugos priemonės:

14.1. siekiant užtikrinti aukštą TIS patikimumą bei jose saugomos ir apdorojamos TIS elektroninės informacijos konfidencialumą, vientisumą ir prieinamumą, turi būti įdiegti duomenų bazių bei rinkmenų tarnybinių stočių klasteriai, viena kitą dubliuojančios užkardos, keli interneto prieigos serveriai, dubliuoti tinklo komutatoriai, patikima duomenų saugykla ir rezervinio kopijavimo įranga;

14.2. visai TIS techninei įrangai privalo būti teikiamas įrangos gamintojų ar jų atstovų suteiktas garantinis aptarnavimas;

14.3. turi būti ribojama fizinė prieiga prie TIS tarnybinių stočių (atskiros rakinamos patalpos);

14.4. patalpose, kuriose yra TIS tarnybinės stotys turi būti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

14.5. TIS kompiuterių aparatinės įrangos keitimas gali būti atliekamas tik Tarnybos Elektroninių pirkimų skyriaus specialistų, gavus šio skyriaus vedėjo nurodymą ar pagal sutartį veikiančių paslaugų teikėjų specialistų;

14.6. TIS kompiuterių aparatinės įrangos gedimai, kai keičiamas vidinis komponentas ar įranga, taisoma specializuotuose taisymo centruose kvalifikuotų specialistų, o TIS įrangos taisymai turi būti registruojami Kompiuterių aparatinės įrangos taisymo ir infrastruktūros pakeitimų žurnale;

14.7. TIS turi perspėti TIS vidaus ir (ar) TIS išorės administratorius, kai tarnybinėse stotyse sumažėja iki pavojingos ribos laisvos operatyviosios atminties ar vietos diske (diskuose) / duomenų saugykloje ar ilgą laiką stipriai apkraunamas centrinis procesorius ir (ar) tinklo sąsaja;

14.8. kompiuterių aparatinė įranga turi būti prižiūrima laikantis gamintojo rekomendacijų.

15. TIS sisteminės ir taikomosios programinės įrangos saugos priemonės:

15.1. TIS tarnybinėse stotyse gali būti naudojama tik legali sisteminė ir taikomoji programinė įranga;

15.2. TIS vidaus naudotojų kompiuterinėje įrangoje turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga; TIS saugos įgaliotinis turi parengti, su TIS valdytojo vadovu suderinti ir ne rečiau kaip kartą per metus peržiūrėti bei prireikus atnaujinti leistinos programinės įrangos sąrašą;

15.3. sisteminės ir taikomosios programinės įrangos apsaugai nuo virusų ir kitų kenkėjiškų programų TIS turi būti naudojama centralizuotai valdoma, specializuota, nuolat automatiškai atnaujinama programinė įranga, stebėjimo realiu laiku priemonės; šios priemonės turi automatiniu būdu informuoti administratorių apie tai, kuriems TIS posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atnaujinimo laikas; TIS komponentai be kenksmingos programinės įrangos aptikimo priemonių gali būti eksploatuojami, jeigu rizikos vertinimo metu yra patvirtinama, kad šių komponentų rizika yra priimtina; ilgiausias leistinas antivirusinės programinės įrangos neatnaujinimo laikas — ne ilgiau kaip 5 darbo dienos;

15.4. kiekvienas TIS vidaus ir išorės naudotojas, TIS vidaus ir išorės administratorius turi būti unikaliai identifikuojamas, todėl visiems TIS vidaus ir išorės naudotojams, TIS vidaus ir išorės

administratoriams, vadovaujantis kiekvienai TIS nustatyta tvarka, nurodyta dokumente „Viešųjų pirkimų tarnybos informacinės sistemos naudotojų vardų ir slaptažodžių sudarymo bei naudojimo taisyklės“, suteikiami TIS vidaus ir išorės naudotojo, TIS vidaus ir išorės administratoriaus vardai bei nustatomi reikalavimai TIS vidaus ar išorės naudotojo, ar vidaus ir išorės administratoriaus tapatybę patvirtinantiems slaptažodžiams, su taisyklėmis naudotojai gali susipažinti Tarnybos intraneto tinklapyje;

15.5. TIS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą TIS vidaus ir išorės administratoriaus identifikatorių, kuriuo naudojantis nebūtų galima atlikti TIS vidaus ar išorės naudotojo funkcijų;

15.6. slaptažodžiai, suteikiantys teisę administruoti TIS bei TIS vidinius ar išorinius naudotojus, žinomi tiktai atitinkamiems TIS vidaus ir išorės administratoriams. Tam, kad nesant administratoriaus atitinkamą sistemą bei jos naudotojus galėtų administruoti jį pavaduojantis darbuotojas, vidaus ir išorės administratorių slaptažodžiai saugomi Tarnybos Elektroninių pirkimų skyriaus vedėjo seife. Perėmus sistemos administravimą pagrindiniam TIS vidaus ar išorės administratoriui, sistemos administratoriaus slaptažodį privaloma pakeisti nauju;

15.7. TIS vidaus ar išorės naudotojui teisė dirbti su konkrečia TIS elektronine informacija turi būti ribojama ar sustabdoma, kai naudotojas atostogauja, nušalinus naudotoją nuo pareigų ir pan.;

15.8. TIS vidaus ar išorės naudotojui teisė naudotis TIS turi būti panaikinta pasibaigus tarnybos (darbo) santykiams;

15.9. TIS vidaus ar išorės naudotojui baigus darbą turi būti imamasi priemonių, kad su TIS elektronine informacija negalėtų susipažinti pašaliniai asmenys:

15.9.1. atsijungiama nuo TIS;

15.9.2. įjungiama ekrano užsklanda su slaptažodžiu;

15.10. TIS vidaus ar išorės naudotojui neatliekant jokių veiksmų, sistema turi taip užsirakinti, kad toliau ja naudotis galima būtų tik pakartojus tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus. Terminas, per kurį TIS vidaus ar išorės naudotojui neatliekant jokių veiksmų TIS turi užsirakinti, negali būti ilgesnis nei 15 min;

15.11. TIS vidaus naudotojų darbo vietose gali būti naudojamos tik tarnybinėms reikmėms skirtos išorinės duomenų laikmenos (pvz., USB, CD, DVD ir kt.). Šios laikmenos negali būti naudojamos veiklai, nesusijusiai su teisėtu TIS tvarkymu.

15.12. visi TIS kompiuterių sisteminės ir taikomosios programinės įrangos keitimai bei atnaujinimai turi būti registruojami „Kompiuterių aparatinės įrangos taisymo ir infrastruktūros pakeitimų žurnale“.

16. TIS elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

16.1. siekiant užtikrinti TIS elektroninės informacijos konfidencialumą ir vientisumą informacijos teikimas bei priėmimas turi būti vykdomas naudojant saugų valstybinį duomenų perdavimo tinklą arba kitą saugų šifruotą duomenų perdavimo kanalą;

16.2. duomenys, siunčiami per viešuosius tinklus, turi būti šifruojami;

16.3. TIS nuo grėsmių iš interneto turi būti atskirtos užkardomis - ugniasienėmis;

16.4. viešai prieinama TIS elektroninė informacija turi būti saugoma atskirame kompiuterių potinklyje.

17. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

17.1. TIS tarnybinės stotys ir kita TIS infrastruktūra bei ją palaikančios sistemos (tikslios klimato kontrolės įrenginiai, ryšio įranga, duomenų perdavimo įranga, apsaugos, signalizacijos ir stebėjimo sistemos) turi būti fiziškai apsaugotos nuo nesankcionuotos prieigos, vagystės, sugadinimo ar sunaikinimo, todėl turi būti eksploatuojama atskirose patalpoje – Tarnybos duomenų centre (toliau – Tarnybos DC), kurio schema nurodyta 1 priede;

17.2. Tarnybos DC turi atitikti šiuos reikalavimus:

17.2.1. Tarnybos DC patalpos atskirtos nuo bendrojo naudojimo patalpų;

17.2.2. apsauga nuo nesankcionuoto patekimo į Tarnybos DC patalpą – turi atitikti standarto EN1627 WK4 reikalavimus;

17.2.3. atsparumas ugniai pagal standarto EN1047-2 reikalavimus – esant Tarnybos DC patalpos išorėje temperatūrai iki 1100 °C, po 30 min. temperatūra šios patalpos viduje neturi viršyti 70 °C;

17.2.4. atsparumas vandeniui pagal standarto EN60529 reikalavimus – ne mažiau 30 min gaisrą Tarnybos DC patalpos išorėje gesinant vandeniu;

17.2.5. atsparumas dulkėms – turi atitikti standarto EN60529 IP56 reikalavimus;

17.2.6. siekiant užtikrinti TIS elektroninės informacijos konfidencialumą Tarnybos DC patalpa turi užtikrinti elektromagnetinio spinduliavimo slopinimą ne mažiau kaip 100 dB elektriniam laukui dažnių juostoje 14 kHz – 10 GHz bei magnetiniam laukui dažnių juostoje 100 kHz – 10 GHz;

17.2.7. turi būti palaikoma 21°C±1°C aplinkos temperatūra bei 60% ±15% drėgnumas. Šiems aplinkos parametrams užtikrinti turi būti sumontuoti dubliuoti tikslios klimato kontrolės įrenginiai;

17.2.8. apsaugai nuo gaisro privalo būti įrengta nepriklausoma Tarnybos DC patalpos gaisrinė signalizacija ir automatinė dujinė (dujos FM200) gaisro gesinimo sistema;

17.3. elektros energija Tarnybos DC eksploatuojamai kompiuterių aparatinei įrangai ir palaikančioms sistemoms turi būti tiekiama atskiru kabeliu per automatinę sistemą, užtikrinančią rezervinį elektros energijos tiekimą ne mažiau kaip 1 (vieną) valandą iš autonominio dyzelinio generatoriaus, nutrūkus pagrindiniam elektros energijos tiekimui;

17.4. Tarnybos DC durys turi būti nedegios, atsparios laužimui, rakinamos elektromagnetiniu užraktu, valdomu įeigos kontrolės sistema su kortelių skaitytuvais;

17.5. patekimas į Tarnybos DC turi būti kontroliuojamas, registruojami įeinančių asmenų apsilankymai bei šių apsilankymų tikslas. Registravimo žurnalo forma nurodyta 2 priede;

17.6. Tarnybos DC draudžiama likti vienam asmeniui;

17.7. į Tarnybos DC gali patekti tik tie asmenys, kuriems tai būtina atliekant darbo funkcijas;

17.8. Tarnybos direktorius įsakymu turi patvirtinti darbuotojų sąrašą, kuriems suteikiamos kortelės, leidžiančios patekti į Tarnybos DC;

17.9. trečiųjų šalių atstovai į Tarnybos DC gali patekti ir dirbti jame tik lydimi Tarnybos Elektroninių pirkimų skyriaus darbuotojo;

17.10. techninė įranga įnešama ir išnešama iš Tarnybos DC patalpų tik gavus raštišką Tarnybos Elektroninių pirkimų skyriaus vedėjo leidimą;

17.11. Tarnybos DC patalpose turi būti įrengta vaizdo stebėjimo sistema su archyvavimo įranga.

17.12. Patekimas į patalpas, kuriose saugomos atsarginės kopijos, turi būti kontroliuojamas.

17.13. Patekimas prie vidinių TIS naudotojų kompiuterinės darbo vietos turi būti kontroliuojamas.

18. Darbo apskaitos ir kitos TIS elektroninės informacijos saugos priemonės:

18.1. TIS tarnybinių stočių įvykių žurnaluose programiniu būdu turi būti registruojami ir ne mažiau kaip 1 (vienerius) metus saugomi duomenys (Tarnybos internetinio tinklo kataloge), nurodant įvykio laiką ir TIS naudotojo identifikatorių, apie:

18.1.1. TIS įjungimą bei išjungimą;

18.1.2. sėkmingus ir nesėkmingus bandymus registruotis TIS;

18.1.3. bandymus prieiti prie TIS elektroninės informacijos;

18.1.4. kitus svarbius saugomos ir apdorojamos TIS elektroninės informacijos saugai įvykius.

III. SAUGUS TIS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

19. TIS elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

19.1. TIS elektroninės informacijos keitimą, atnaujinimą, įvedimą ir naikinimą gali atlikti tik tam turintys teisę autorizuoti TIS vidaus ir išorės naudotojai;

19.2. TIS elektroninė informacija saugoma, apdorojama, įvedama, atnaujinama, keičiama ir naikinama vadovaujantis Lietuvos Respublikos teisės aktais ir Duomenų saugos nuostatais.

20. TIS vidaus ir (ar) išorės naudotojų veiksmų registravimo tvarka:

20.1. siekiant nustatyti neteisėtus veiksmus su TIS elektronine informacija bei šios informacijos vientisumo pažeidimus naudotojų veiksmai, jų darbo su TIS laikas turi būti automatiškai registruojami elektroniniuose žurnaluose, apsaugotuose nuo neteisėto jame esančių duomenų panaudojimo, pakeitimo, iškraipymo ar sunaikinimo;

20.2. veiksmų žurnalų duomenys turi būti prieinami tik atitinkamas teises turintiems TIS vidaus ir išorės administratoriams.

21. TIS elektroninės informacijos kopijų darymo, saugojimo ir TIS elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka nustatyta TIS saugos nuostatuose ir dokumente „Viešųjų pirkimų tarnybos informacinių sistemų atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka“.

22. Saugaus TIS elektroninės informacijos perkėlimo ir teikimo susijusioms informacinėms sistemoms, TIS elektroninės informacijos gavimo iš jų užtikrinimo tvarka:

22.1. TIS elektroninė informacija kitoms sistemoms teikiama ir (ar) gaunama iš jų su šių sistemų valdytojais sudarytose duomenų teikimo sutartyse numatytais būdais, apimtimi, reguliarumu ir (ar) terminais;

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

23.1. TIS vidaus ir išorės administratoriai, užtikrindami TIS elektroninės informacijos saugą, privalo naudoti visas įmanomas aparatines, programines ir administracines priemones skirtas apsisaugojimui nuo neleidžiamos veiklos;

23.2. siekiant patikrinti ar su TIS elektronine informacija nėra vykdoma neleidžiama veikla, TIS vidaus ir išorės administratoriai kiekvieną darbo dieną privalo peržiūrėti TIS programinės įrangos elektroniniuose žurnaluose sukauptus atitinkamus įrašus;

23.3. TIS vidaus ar išorės naudotojas, įtaręs, kad su TIS elektronine informacija buvo atlikti neteisėti veiksmai, privalo pranešti apie tai TIS vidaus administratoriams;

23.4. Vidaus administratoriai, atsiradus įtarimams dėl neteisėtų veiksmų su TIS elektronine informacija, pasinaudoję elektroniniuose žurnaluose sukauptais įrašais, nustato neteisėto poveikio šaltinį, laiką ir veiksmus, atliktus su TIS programine įranga ir (ar) TIS elektronine informacija;

23.5. kilus įtarimui, kad su TIS ir (ar) TIS elektronine informacija yra vykdoma neleidžiama veikla, TIS vidaus ir (ar) išorės administratoriai nedelsiant privalo apie tai informuoti TIS saugos įgaliotinį;

23.6. TIS saugos įgaliotinis, gavęs pranešimą apie neleidžiamą veiklą inicijuoja TIS elektroninės informacijos saugos incidentų valdymo procedūros vykdymą.

24. Mobiliuosiuose įrenginiuose (nešiojamuosiuose kompiuteriuose, planšetėse, išmaniuosiuose telefonuose ir pan.), jeigu jie naudojami ne duomenų valdytojo ir (ar) duomenų tvarkytojo vidiniame kompiuterių tinkle, esantys ypatingi asmens duomenys ir prisijungimo prie duomenų valdytojo ir (ar) duomenų tvarkytojo tvarkomų asmens duomenų informacija šifruojama, privaloma naudoti papildomas saugos priemones, kuriomis patvirtinama naudotojo tapatybė (PIN kodas ir pan.) Iš visų kompiuterių, kurie perduodami taisyti ar techninei priežiūrai atlikti, turi būti išimti standieji diskai bei pašalinta visa kitose laikmenose esanti TIS elektroninė informacija.

25. Sugedę standieji diskai ir nusidėvėjusios magnetinės atsarginio kopijavimo laikmenos turi būti neatstatomai sunaikintos ir atiduotos perdirbimui. Laikmenų sunaikinimas turi būti įforminamas aktu.

26. Pokyčių valdymo tvarka:

26.1. TIS valdytojas užtikrina TIS pokyčių valdymo planavimą, apimantį pokyčių identifikavimą, suskirstymą į kategorijas pagal pokyčio tipą (administracinis, organizacinis ar

techninis), įtakos vertinimą (skubumas ir svarbumas), pokyčių prioritetų nustatymo (eiliškumas) procesus;

26.2. pokyčiai identifikuojami (projektavimas, kūrimas, testavimas, diegimas) atliekami tik TIS valdytojo iniciatyva, TIS saugos įgaliotinio iniciatyva ar TIS vidaus ir (ar) išorės administratorių iniciatyva;

26.3. pokyčių projektavimą ir kūrimą atlieka TIS vidaus ir (ar) išorės administratorius tam skirtoje kūrimo aplinkoje. Atlikdamas pakeitimo projektavimą ir kūrimą, TIS vidaus ir (ar) išorės administratorius gali pasitelkti trečiąsias šalis;

26.4. prieš atliekant pokyčius, kurių metu gali iškilti grėsmė TIS elektroninės informacijos konfidencialumui, vientisumui ar pasiekiamumui, visi pokyčiai turi būti išbandomi testavimo aplinkoje, kuri yra identiška gamybinei aplinkai;

26.5. įgyvendinant pokyčius, kurių metu galimi TIS veikimo sutrikimai, TIS vidaus ir (ar) išorės administratorius privalo ne vėliau kaip prieš dvi darbo dienas iki planuojamų pokyčių pradžios (el. paštu, faksu ar kitomis priemonėmis) informuoti TIS tvarkymo įstaigų vidaus ir (ar) išorės administratorius ir TIS vidaus ir (ar) išorės naudotojus apie tokių darbų pradžią ir galimus sutrikimus;

26.6. atlikęs pokyčių testavimą, jei ir testavimo darbų dėl programinių ir (ar) techninių priežasčių nebuvo galima atlikti, TIS vidaus ir (ar) išorės administratorius gali pradėti eksploatuoti pakeitimus;

26.7. jeigu testavimai sėkmingi pokyčiai perkeliami į gamybinę aplinką;

26.8. visi pokyčiai registruojami ir apie tai informuojami TIS vidaus ir (ar) išorės administratoriai ir TIS vidaus ir (ar) išorės naudotojai.

27. Pokyčiai, galintys daryti neigiamą įtaką TIS elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui turi būti patikrinti bandomojoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo eksploatuojamos informacinės sistemos.

28. Programinė įranga turi būti testuojama naudojant atskirą testavimui skirtą aplinką, kurioje esantys asmens duomenys turi būti naudojami vadovaujantis Bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonių, patvirtintų Valstybinės duomenų apsaugos inspekcijos direktoriaus 2008 m. lapkričio 12 d. įsakymu Nr. 1T-71 (1.12) „Dėl bendrųjų reikalavimų organizacinėms ir techninėms asmens duomenų saugumo priemonėms patvirtinimo“, reikalavimais.

IV. REIKALAVIMAI, KELIAMI INFORMACINĖMS SISTEMOMS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TIEKĖJAMS

29. TIS priežiūros paslaugų teikėjams suteikiami tokie prieigos prie TIS lygiai ir sąlygos, kurie reikalingi ir pakankami atliekamoms pagal sutartį priežiūros paslaugoms atlikti.

30. Reikalavimai TIS priežiūros paslaugoms nurodyti dokumente „Informacinių sistemų priežiūros paslaugos techninė specifikacija“.

31. Reikalavimai interneto ryšio teikimo paslaugai nurodyti dokumente „Interneto ryšio paslaugos techninė specifikacija“.

32. Reikalavimai paslaugų tiekėjams nurodyti dokumente „Kvalifikaciniai reikalavimai IT paslaugų tiekėjams“.

V. BAIGIAMOSIOS NUOSTATOS

33. Asmenys, pažeidę TIS elektroninės informacijos saugą reglamentuojančių dokumentų ir kitų saugų TIS elektroninės informacijos tvarkymą reglamentuojančių teisės aktų nuostatas, atsako teisės aktų nustatyta tvarka.

_____

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018 m. rugsėjo 25 d. raštu Nr. (4.2)6K-599

PATVIRTINTA
Viešųjų pirkimų tarnybos
direktoriaus 2018 m. lapkričio 26 d.
įsakymu Nr. 1S-158

VIEŠŲJŲ PIRKIMŲ TARNYBOS INFORMACINIŲ SISTEMŲ VEIKLOS TĘSTINUMO VALDYMO PLANAS

I. BENDROSIOS NUOSTATOS

1. Viešųjų pirkimų tarnybos informacinių sistemų veiklos tęstinumo valdymo plano (toliau – Valdymo planas) tikslas – nustatyti Viešųjų pirkimų tarnybos (toliau – Tarnybos) informacinių sistemų: Centrinės viešųjų pirkimų informacinės sistemos, Viešųjų pirkimų rizikos valdymo informacinės sistemos ir Vidaus administravimo informacinės sistemos (toliau visos kartu – TIS) vidaus ir išorės naudotojų, TIS saugos įgaliotinio, TIS vidaus ir išorės administratorių – veiksmus įvykus TIS elektroninės informacijos saugos incidentui, kurios metu gali kilti pavojus TIS elektroninei informacijai (gali būti pažeistas duomenų vientisumas, konfidencialumas ar prieinamumas), TIS tarnybinių stočių aparatinės ir programinės įrangos bei kompiuterizuotų darbo vietų (toliau – KDV) funkcionavimui, gali būti pažeistas TIS elektroninės informacijos teikimas suinteresuotiems juridiniams bei fiziniams asmenims ir (arba) jų valdomoms informacinėms sistemoms, gali būti pažeistas elektroninės informacijos priėmimas iš suinteresuotų juridinių bei fizinių asmenų ir (arba) jų valdomų informacinių sistemų.

2. Valdymo planas parengtas vadovaujantis šiais teisės aktais:

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

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

2.3. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V–832 „Dėl Techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

2.4. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas, patvirtintas 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“;

3. Valdymo plane vartojamos sąvokos:

3.1. **Tarnybos informacinės sistemos (TIS)** – Tarnybos Centrinė viešųjų pirkimų informacinė sistema (toliau – CVP IS), Tarnybos Viešųjų pirkimų rizikos valdymo informacinė sistema (toliau – VPRV IS) ir Tarnybos Vidaus administravimo informacinė sistema (toliau – VA IS).

3.2. **TIS išorės administratorius** – asmuo, pagal Tarnybos pasirašytą paslaugų teikimo sutartį, atliekantis TIS priežiūrą.

3.3. **TIS išorės naudotojas (pagal įstatymą) –** asmuo, kuris nėra Tarnybos Darbuotojas, tačiau, vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymu, Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymu, Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymu, Lietuvos Respublikos koncesijų įstatymu turi teisę naudotis TIS ištekliais Viešųjų pirkimų įstatyme, Gynybos įstatyme, Pirkimų įstatyme bei Koncesijų įstatyme numatytoms funkcijoms atlikti.

3.4. **TIS išorės naudotojas (pagal sutartį)** – asmuo, kuris nėra Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, bet pagal Tarnybos pasirašytą duomenų teikimo sutartį, turintis teisę naudotis TIS ištekliais duomenų teikimo sutartyje ar teisės aktuose numatytoms funkcijoms atlikti.

3.5. **TIS vidaus administratorius** – Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atliekantis TIS priežiūrą.

3.6. **TIS vidaus naudotojas** – Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis TIS ištekliais numatytoms darbo ar valstybės tarnybos funkcijoms atlikti.

4. Kitos Valdymo plane naudojamos sąvokos atitinka šio plano 2 punkte nurodytuose teisės aktuose nustatytas sąvokas.

5. Planas pradedamas vykdyti įvykus TIS elektroninės informacijos saugos incidentui.

6. Valdymo planas yra privalomas TIS tvarkytojams, TIS valdytojui, TIS saugos įgaliotiniui, TIS duomenų valdymo įgaliotiniui, TIS vidaus ir išorės administratoriams ir TIS vidaus ir išorės naudotojams. Valdymo plano įgyvendinimas turi užtikrinti CVP IS prieinamumą ne mažiau kaip 96 proc. laiko per parą bei CVP IS veiklos atnaujinimą per 1 val., VPRV IS ir VA IS prieinamumą ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis bei VPRV IS ir VA IS veiklos atnaujinimą per 8 val.

7. Už Valdymo plano įgyvendinimą atsakingi Tarnybos direktoriaus įsakymu paskirti Tarnybos darbuotojai.

8. Už Valdymo plano įgyvendinimo organizavimą ir kontrolę atsakingas Tarnybos direktoriaus pavaduotojas, kuruojantis TIS veiklą.

9. TIS Saugos įgaliotinio, TIS vidaus ir išorės administratorių funkcijos ir veiksmai elektroninės informacijos saugos incidento metu nurodyti Viešųjų pirkimų tarnybos informacinių sistemų veiklos atkūrimo detaliajame plane (toliau – Detalusis planas) (1 priedas).

10. Reikalavimai, keliami atsarginėms patalpoms, naudojamoms informacinės sistemos veiklai atkurti įvykus TIS elektroninės informacijos saugos incidentui, atsarginių patalpų adresas ir būdai, kaip iki jų nuvykti nurodyti Viešųjų pirkimų tarnybos informacinių sistemų atsarginių elektroninės informacijos kopijų darymo, saugojimo ir elektroninės informacijos atkūrimo iš atsarginių kopijų tvarkoje.

11. Kriterijai, pagal kuriuos nustatoma, kad TIS veikla atkurta, yra:

11.1. TIS elektroninės informacijos centro aparatinė ir programinė įranga bei KDV funkcionuoja pagal specifikacijoje nustatytus reikalavimus;

11.2. nuolat priimama ir išsaugoma suinteresuotų juridinių bei fizinių asmenų ir (arba) jų valdomų informacinių sistemų siunčiama elektroninė informacija;

11.3. išsaugoma atnaujinta TIS elektroninė informacija;

11.4. nuolat teikiama atnaujinta TIS elektroninė informacija suinteresuotiems juridiniams bei fiziniams asmenims ir (arba) jų valdomoms informacinėms sistemoms;

11.5. užtikrinamas TIS elektroninės informacijos vientisumas, konfidencialumas ir prieinamumas;

11.6. atliekamas TIS elektroninės informacijos rezervinis kopijavimas.

II. ORGANIZACINĖS NUOSTATOS

12. TIS veiklos tęstinumo valdymo grupės (toliau – Valdymo grupė) sudėtis:

12.1. Valdymo grupės vadovas – Tarnybos direktorius;

12.2. Valdymo grupės vadovo pavaduotojas – Elektroninių pirkimų skyriaus vedėjas;

12.3. Valdymo grupės narys – TIS saugos įgaliotinis;

12.4. Valdymo grupės narys –TIS duomenų valdymo įgaliotinis (-iai);

12.5. Valdymo grupės nariai – kiti Tarnybos direktoriaus įsakymu paskirti valstybės tarnautojai arba juridinių asmenų atstovai, veikiantys pagal su Tarnyba sudarytą sutartį.

13. Valdymo grupės funkcijos:

13.1. situacijos analizė ir sprendimų TIS veiklos tęstinumo valdymo klausimais priėmimas;

13.2. bendravimas su viešosios informacijos rengėjų ir viešosios informacijos skleidėjų atstovais;

13.3. bendravimas su susijusių informacinių sistemų veiklos tęstinumo valdymo grupėmis;

13.4. bendravimas su teisėsaugos ir kitomis institucijomis, institucijų darbuotojais ir kitomis interesų grupėmis;

13.5. finansinių ir kitų išteklių, reikalingų informacinės sistemos veiklai atkurti, įvykus TIS elektroninės informacijos saugos incidentui, naudojimo kontrolė;

13.6. TIS elektroninės informacijos fizinė sauga įvykus TIS elektroninės informacijos saugos incidentui;

13.7. logistika (žmonių, daiktų, įrangos gabenimo organizavimas ir gabenimas);

13.8. TIS veiklos atkūrimo priežiūra ir koordinavimas;

13.9. kitos Tarnybos vadovybės Valdymo grupei pavestos funkcijos;

13.10. Tarnybos darbuotojų KDV veikimo atkūrimo ir funkcionavimo Tarnybos kompiuterių tinkle organizavimas.

14. TIS veiklos atkūrimo grupės (toliau – Atkūrimo grupė) sudėtis:

14.1. Atkūrimo grupės vadovas – Tarnybos direktoriaus pavaduotojas, kuruojantis TIS veiklą;

14.2. Atkūrimo grupės vadovo pavaduotojas – Elektroninių pirkimų skyriaus vyriausiasis specialistas;

14.3. Atkūrimo grupės narys – TIS vidaus administratorius;

14.4. Atkūrimo grupės nariai – kiti Tarnybos direktoriaus įsakymu paskirti valstybės tarnautojai arba juridinių asmenų atstovai, veikiantys pagal su Tarnyba sudarytą sutartį.

15. Atkūrimo grupės funkcijos:

15.1. TIS tarnybinių stočių veikimo atkūrimo organizavimas;

15.2. kompiuterių tinklo ir interneto ryšio veikimo atkūrimo organizavimas;

15.3. TIS elektroninės informacijos atkūrimo organizavimas;

15.4. TIS taikomųjų programų tinkamo veikimo atkūrimo organizavimas;

15.5. kitos Tarnybos vadovybės Atkūrimo grupei pavestos funkcijos.

16. TIS veiklos tęstinumo valdymo ir TIS veiklos atkūrimo grupių nariai turi reaguoti ir valdyti saugos incidentus, vadovaudamiesi 1 priede pateiktomis instrukcijomis.

17. TIS vidaus ir išorės naudotojai, vidaus ir išorės administratoriai, Tarnybos Administravimo skyriaus vedėjas, priklausomai nuo grėsmės sukėlusios TIS elektroninės informacijos saugos incidentą, nedelsdami informuoja TIS saugos įgaliotinį.

18. TIS saugos įgaliotinis apie TIS elektroninės informacijos saugos incidentą nedelsdamas informuoja Valdymo grupės vadovą, Atkūrimo grupės vadovą ir registruoja nenumatytą situaciją TIS nenumatytų situacijų registravimo žurnale (2 priedas).

19. Valdymo grupės vadovas organizuoja nenumatytos situacijos įvertinimą ir priima sprendimą dėl Detaliojo plano vykdymo. Priimdama šį sprendimą Valdymo grupė vadovaujasi kriterijais:

19.1. ar nenumatytos situacijos padarinių likvidavimui bus reikalingi papildomi finansiniai ištekliai;

19.2. ar bus reikalingas TIS elektroninės informacijos atstatymas iš rezervinių kopijų;

19.3. ar reikalingas teisėsaugos institucijų informavimas.

20. Tuo atveju, kai nevykdomas Detalusis planas Elektroninių pirkimų skyriaus vedėjas, Administravimo skyriaus vedėjas ir (ar) TIS vidaus ir išorės administratoriai atkuria TIS veiklą ir informuoja Valdymo grupės vadovą. Elektroninių pirkimų skyriaus vedėjas, Administravimo skyriaus vedėjas įvertina ar pašalinti nenumatytos situacijos sukelti padariniai. Jeigu nenumatytos situacijos sukelti padariniai pašalinti - TIS saugos įgaliotinis tai pažymi TIS elektroninės informacijos saugos incidentų registravimo žurnale (2 priedas).

21. Tuo atveju, kai vykdomas Detalusis planas, jo vykdymui vadovauja Tarnybos direktoriaus pavaduotojas – Atkūrimo grupės vadovas. Kitų Grupės narių funkcijos, atsakomybės bei sąveika nurodyti Detaliajame plane.

22. Atkūrus TIS veiklą Atkūrimo grupė įvertina, ar pašalinti TIS elektroninės informacijos saugos incidento sukelti padariniai. Jeigu padariniai pašalinti – TIS saugos įgaliotinis tai pažymi TIS elektroninės informacijos saugos incidentų registravimo žurnale (2 priedas).

23. Atkūrimo grupėms priklausantys Tarnybos darbuotojai tarpusavyje sąveikauja ir komunikuoja bet kuriomis, TIS elektroninės informacijos saugos incidento metu veikiančiomis ryšio priemonėmis (elektroniniu paštu, fiksuoto ir judriojo ryšio telefonais).

24. TIS elektroninės informacijos saugos incidento metu pažeista, sugadinta arba sunaikinta TIS tarnybinių stočių aparatinė, ir programinė įranga bei KDV įranga atstatoma arba įsigyjama Viešųjų pirkimų įstatymo nustatyta tvarka, įsigijimo finansiniai ištekliai padengiami iš valstybės biudžeto.

25. Atsarginių patalpų, naudojamų veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, reikalavimai:

25.1. patekimas į patalpas turi būti registruojamas žurnale;

25.2. patalpos turi būti atskirtos nuo bendrojo naudojimo patalpų;

25.3. patalpos turi atitikti priešgaisrinės saugos reikalavimus, jose turi būti įrengtos gaisro gesinimo priemonės;

25.4. patalpų durys turi būti šarvuotos ir apsaugotos bent dviem skirtingos konstrukcijos spynomis;

25.5. patalpose turi būti įrengtas rezervinis elektros energijos šaltinis užtikrinantis įrangos veikimą ne trumpiau kaip 30 minučių;

25.6. patalpoje turi nuolat veikti oro temperatūros ir drėgmės reguliavimo įranga (oro kondicionavimo sistema).

25.7. Atsarginių patalpų, naudojamų TIS veiklai atkurti, įvykus elektroninės informacijos saugos incidentui, adresas ir, kaip jas rasti, nurodyta 3 priede.

III. APRAŠOMOSIOS NUOSTATOS

26. Parengtų ir saugomų dokumentų sąrašas, saugomas TIS Saugos įgaliotinio kabinete:

26.1. TIS informacinių technologijų įrangos sąrašų ir jų parametrų dokumentacija;

26.2. informacinių technologijų įrangos parametrų dokumentacija ir už šios įrangos priežiūrą atsakingų administratorių sąrašas. TIS administratorių pavaduojančio asmens minimalus kompetencijos ar žinių lygis negali būti žemesnis už TIS administratoriui keliamų reikalavimų lygį.

26.3. specifikacija, kurioje nurodyti minimalaus funkcionalumo informacinių technologijų įrangos, tinkamos institucijos poreikius atitinkančiai informacinės sistemos veiklai užtikrinti įvykus elektroninės informacijos saugos incidentui parametrai;

26.4. Duomenų centro patalpų, kuriose yra TIS įranga ir komunikacijos, brėžinius ir šiose patalpose esančios įrangos sąrašas. Patalpų brėžiniuose pažymima:

26.4.1. tarnybinės stotys;

26.4.2. kompiuterių tinklo ir telefonų tinklo mazgai;

26.4.3. kompiuterių tinklo ir telefonų tinklo laidų vedimo tarp pastato aukštų vietos;

26.4.4. elektros įvedimo pastate vietos.

26.5. kompiuterių tinklo fizinio ir loginio sujungimo schemų dokumentacija;

26.6. elektroninės informacijos teikimo ir kompiuterinės, techninės ir programinės įrangos priežiūros sutarčių ir atsakingų už šių sutarčių įgyvendinimo priežiūrą asmenų (nurodant pareigas) sąrašas;

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

26.8. sąrašas, kuriame nurodyti veiklos tęstinumo valdymo grupės ir veiklos atkūrimo grupės nariai su kontaktiniais duomenimis, leidžiančiais pasiekti šiuos asmenis bet kuriuo metu;

26.9. Viešųjų pirkimų tarnybos informacinių sistemų duomenų saugos nuostatai.

26.10. Viešųjų pirkimų tarnybos informacinių sistemų saugaus TIS elektroninės informacijos tvarkymo taisyklės.

26.11. Viešųjų pirkimų tarnybos informacinių sistemų veiklos tęstinumo valdymo planas.

26.12. Viešųjų pirkimų tarnybos informacinių sistemų naudotojų administravimo taisyklės.

26.13. Viešųjų pirkimų tarnybos informacinių sistemų atsarginių TIS elektroninės informacijos kopijų darymo, saugojimo ir TIS elektroninės informacijos atkūrimo iš atsarginių kopijų tvarka.

26.14. Viešųjų pirkimų tarnybos informacinių sistemų administratorių ir naudotojų vardų ir slaptažodžių sudarymo bei naudojimo taisyklės.

26.15. už Valdymo plano 25 punkte nurodytų dokumentų parengimą ir saugojimą atsakingas Saugos įgaliotinis.

IV. VALDYMO PLANO VEIKSMINGUMO IŠBANDYMO NUOSTATOS

27. Valdymo plano veiksmingumas išbandomas ne rečiau kaip vieną kartą per metus.

28. Valdymo plano išbandymo būdas ir data, atsižvelgiant per praėjusius kalendorinius metus įvykusius TIS elektroninės informacijos saugos incidentus, užfiksuotus TIS elektroninės informacijos saugos incidentų registravimo žurnale, TIS saugos įgaliotinio teikimu, tvirtinami Valdymo grupės posėdyje.

29. TIS saugos įgaliotinis per 10 darbo dienų po Valdymo plano veiksmingumo išbandymo parengia išbandymo ataskaitą bei priemonių planą išbandymo metu pastebėtiems trūkumams pašalinti.

30. Valdymo plano veiksmingumo išbandymo ataskaitą bei priemonių pastebėtiems trūkumams pašalinti planą, pritarus Atkūrimo grupei, tvirtina Tarnybos direktorius.

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

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018 m. rugsėjo 25 d. raštu Nr. (4.2)6K-599

PATVIRTINTA
Viešųjų pirkimų tarnybos
direktoriaus 2018 m. lapkričio 26 d.
įsakymu Nr. 1S-158

VIEŠŲJŲ PIRKIMŲ TARNYBOS INFORMACINIŲ SISTEMŲ NAUDOTOJŲ ADMINISTRAVIMO TAISYKLĖS

I. BENDROSIOS NUOSTATOS

1. Viešųjų pirkimų tarnybos informacinių sistemų naudotojų administravimo taisyklės (toliau – Taisyklės) nustato tvarką ir principus, kuriais vadovaujantis Viešųjų pirkimų tarnybos (toliau – Tarnyba) Centrinės viešųjų pirkimų informacinės sistemos, Tarnybos Vidaus administravimo informacinės sistemos ir Tarnybos Viešųjų pirkimų rizikos valdymo informacinės sistemos vidaus ir išorės administratoriai suteikia ar panaikina šių informacinių sistemų naudotojams prieigą prie šių informacinių sistemų bei suteikia, koreguoja ar panaikina teises naudotis šiose informacinėse sistemose tvarkomais duomenimis.

2. Taisyklės parengtos vadovaujantis šiais teisės aktais:

2.1. Bendrųjų elektroninės informacijos saugos reikalavimų aprašu, Saugos dokumentų turinio gairių aprašu ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo 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 elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“;

2.2. Techniniais valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimais, patvirtintais Lietuvos Respublikos vidaus reikalų ministro 2013 m. spalio 4 d. įsakymu Nr. 1V-832 „Dėl techninių valstybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų patvirtinimo“;

2.3. Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų ypatingos svarbos informacinei infrastruktūrai ir valstybės informaciniams ištekliams, aprašas, patvirtintas 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“.

3. Taisyklėse vartojamos sąvokos:

3.1. Tarnybos informacinės sistemos (TIS) – Tarnybos Centrinė viešųjų pirkimų informacinė sistema, Tarnybos Vidaus administravimo informacinė sistema ir Tarnybos Viešųjų pirkimų rizikos valdymo informacinė sistema.

3.2. TIS Vidaus administratorius – Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atliekantis TIS priežiūrą.

3.3. TIS išorės administratorius – asmuo, pagal Tarnybos pasirašytą paslaugų teikimo sutartį, atliekantis TIS priežiūrą.

3.4. TIS vidaus naudotojas – Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, turintis teisę naudotis TIS ištekliais numatytoms darbo ar valstybės tarnybos funkcijoms atlikti.

3.5. TIS išorės naudotojas (pagal sutartį) – asmuo, kuris nėra Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, bet pagal Tarnybos pasirašytą duomenų

teikimo sutartį, turintis teisę naudotis TIS ištekliais duomenų teikimo sutartyje ar teisės aktuose numatytoms funkcijoms atlikti.

3.6. TIS išorės naudotojas (pagal įstatymą) – asmuo, kuris nėra Tarnybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, tačiau vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymu, Lietuvos Respublikos viešųjų pirkimų, atliekamų gynybos ir saugumo srityje, įstatymu, Lietuvos Respublikos pirkimų, atliekamų vandentvarkos, energetikos, transporto ar pašto paslaugų srities perkančiųjų subjektų, įstatymu, Lietuvos Respublikos koncesijų įstatymu turi teisę naudotis TIS ištekliais įstatyme numatytoms funkcijoms atlikti.

Kitos Taisyklėse vartojamos sąvokos atitinka Taisyklių 3 punkte nurodytuose teisės aktuose nustatytas sąvokas.

4. Taisyklės įsigalioja, kai jos, suderinus su Nacionaliniu kibernetinio saugumo centru prie Krašto apsaugos ministerijos ir patvirtinamos Tarnybos direktoriaus įsakymu.

5. Vadovautis Taisyklėmis privalo visi TIS vidaus ir išorės naudotojai, TIS vidaus ir išorės administratoriai, saugos įgaliotinis.

6. Už Taisyklių įgyvendinimą ir jų laikymosi kontrolę atsakingas TIS saugos įgaliotinis.

7. TIS vidaus ir išorės naudotojams prieiga prie TIS tvarkomų duomenų suteikiama vadovaujantis šiais principais:

7.1. TIS vidaus naudotojams prieiga turi būti suteikiama tik prie tų duomenų ir tik tokia apimtimi, kuri reikalinga pareigybės aprašyme nurodytoms funkcijoms atlikti;

7.2. TIS išorės naudotojams (pagal įstatymą) prieiga turi būti suteikiama tik prie tų duomenų ir tik tokia apimtimi, kuri reikalinga Viešųjų pirkimų įstatyme ir kituose viešųjų pirkimų vykdymo tvarką reglamentuojančiuose teisės aktuose nurodytoms funkcijoms atlikti;

7.3. TIS išorės naudotojams (pagal sutartį) prieiga turi būti suteikiama tik prie tų duomenų ir tik tokia apimtimi, kuri nurodyta duomenų teikimo sutartyse;

7.4. TIS tvarkomus duomenis gali tvarkyti (sukurti, papildyti ar panaikinti) tik tokius įgaliojimus turintys TIS naudotojai;

7.5. Prieiga prie TIS saugomų duomenų ir teisė juos apdoroti suteikiama tik TIS vidaus ir išorės naudotojui susipažinus su saugos dokumentais ir pasirašius Taisyklių 1 priedo žurnale „Viešųjų pirkimų tarnybos informacinių sistemų naudotojų supažindinimo su saugos dokumentais žurnalas“.

II. TIS NAUDOTOJŲ IR ADMINISTRATORIŲ ĮGALIOJIMAI, TEISĖS IR PAREIGOS

8. TIS vidaus ir išorės naudotojai gali naudotis tik tomis TIS funkcijomis bei TIS tvarkomais duomenimis, prie kurių prieigą jiems suteikė TIS vidaus ir išorės administratoriai.

9. TIS vidaus ir išorės naudotojai pastebėję TIS saugumo pažeidimus, neleistinos arba nusikalstamos veikos požymius, neveikiančias arba netinkamai veikiančias duomenų saugą užtikrinančias priemones, privalo apie tai nedelsdami pranešti atitinkamos TIS vidaus administratoriui, o pastarasis nedelsdamas informuoti TIS saugos įgaliotinį.

10. TIS vidaus ir išorės naudotojai privalo užtikrinti jų naudojamos TIS elektroninės informacijos konfidencialumą bei vientisumą, savo veiksmais netrikdyti duomenų prieinamumo.

11. TIS vidaus ir išorės naudotojai turi teisę gauti informaciją apie jų naudojamų duomenų apsaugos lygį bei taikomas apsaugos priemones, rekomenduoti papildomas apsaugos priemones.

12. TIS vidaus ir išorės naudotojai, naudodamiesi TIS elektronine informacija, privalo:

12.1. rūpintis TIS ir jose tvarkomos TIS elektroninės informacijos saugumu;

12.2. informuoti TIS vidaus administratorių (-ius) apie TIS elektroninės informacijos saugos incidentus.

13. Kiti TIS vidaus ir išorės naudotojų, TIS vidaus ir išorės administratorių įgaliojimai, teisės ir pareigos yra nustatomi TIS nuostatuose, kituose TIS saugos politiką įgyvendinančiuose dokumentuose bei duomenų teikimo sutartyse.

III. SAUGAUS TIS ELEKTRONINĖS INFORMACIJOS TEIKIMO TIS NAUDOTOJAMS KONTROLĖS TVARKA

14. Už TIS vidaus ir išorės naudotojų prieigos prie atitinkamos TIS ir su tuo susijusių teisių suteikimą, pakeitimą arba panaikinimą yra atsakingi tos TIS vidaus ir (ar) išorės administratoriai.

15. TIS vidaus ir išorės naudotojams negali būti suteikiamos TIS administratoriaus teisės.

16. TIS priežiūros funkcijos turi būti atliekamos naudojant atskirą tam skirtą TIS administratoriaus paskyrą, kuria naudojantis negalima atlikti TIS naudotojo funkcijos.

17. Centrinės viešųjų pirkimų informacinės sistemos (toliau – CVP IS) vidaus naudotojams prieiga prie CVP IS suteikiama tiesioginio vidaus naudotojo vadovo sprendimu elektroniniu paštu informavus apie tai Tarnybos Elektroninių pirkimų skyriaus vedėją.

18. CVP IS išorės naudotojams prieiga prie sistemos suteikiama arba panaikinama:

18.1. išorės naudotojui (pagal sutartį), tik pasirašius duomenų teikimo sutartį ir vadovaujantis tokių sutarčių atitinkamomis nuostatomis arba duomenų valdytojų sudarytais naudotojų teisių reglamentais;

18.2. išorės naudotojui (pagal įstatymą), tik gavus išorės naudotojo (pagal įstatymą) registracijos prašymą arba prašymą panaikinti naudotojo prieigą.

19. Viešųjų pirkimų rizikos valdymo informacinės sistemos (toliau – VPRV IS) vidaus naudotojams prieiga prie sistemos suteikiama arba panaikinama tiesioginio vidaus naudotojo vadovo sprendimu elektroniniu paštu informavus apie tai Tarnybos Elektroninių pirkimų skyriaus vedėją.

20. VPRV IS išorės naudotojams prieiga prie sistemos suteikiama arba panaikinama pasirašius duomenų teikimo susitarimą.

21. Vidaus administravimo informacinės sistemos (toliau – VA IS) vidaus naudotojams prieiga suteikiama arba panaikinama tiesioginio vidaus naudotojo vadovo sprendimu elektroniniu paštu informavus apie tai Elektroninių pirkimų skyriaus vedėją.

22. TIS vidaus ir išorės naudotojų tapatybė nustatoma pagal unikalų naudotojo vardą ir slaptažodį.

23. Reikalavimai TIS vidaus ir išorės administratoriaus, TIS vidaus ir išorės naudotojo vardui ir slaptažodžiui nurodyti Tarnybos TIS administratorių ir naudotojų vardų ir slaptažodžių sudarymo bei naudojimo taisyklėse.

24. Didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius turi būti ne didesnis nei 5 kartai. Įvedus slaptažodį 5 kartus neteisingai, TIS turi užsirakinti ir neleisti identifikuotis ne trumpesnį nei 15 min laiko tarpą.

25. Tarnybos Elektroninių pirkimų skyriaus vedėjo sprendimu TIS vidaus naudotojui teisė dirbti su konkrečia TIS elektronine informacija ribojama ar sustabdoma, kai vidaus naudotojas nedirba ilgiau kaip 3 mėn., nušalinus jį nuo pareigų ir pan. Pasibaigus tarnybos (darbo) santykiams, vidinio informacinės sistemos naudotojo teisė naudotis informacine sistema turi būti panaikinta nedelsiant.

26. Kai TIS vidaus naudotojas perkeliamas į kitas pareigas, jam suteiktos TIS vidaus naudotojo teisės pakeičiamos atsižvelgiant į jo pareigybės aprašyme nurodytas funkcijas.

27. TIS vidaus naudotojui teisė naudotis TIS turi būti panaikinta pasibaigus tarnybos (darbo) santykiams, netekus teisės naudotis TIS elektronine informacija ar nustačius neteisėtą TIS vidaus naudotojo veiką.

28. Nutolusių CVP IS vidaus ir išorės naudotojų prisijungimui naudojamas HTTPS protokolas.

_____

SUDERINTA
Nacionalinio kibernetinio saugumo centro
prie Krašto apsaugos ministerijos
2018 m. rugsėjo 25 d. raštu Nr. (4.2)6K-599