PATVIRTINTA
Valstybinės energetikos reguliavimo
tarybos pirmininko
2020 m. spalio 2 d. įsakymu Nr.O1E-172

VALSTYBINĖS ENERGETIKOS REGULIAVIMO TARYBOS INFORMACIJOS APDOROJIMO PRIEMONIŲ NAUDOJIMO TVARKOS APRAŠAS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybinės energetikos reguliavimo tarybos (toliau – Taryba) informacijos apdorojimo priemonių naudojimo tvarkos aprašas (toliau – Aprašas) nustato:

1.1. Tarybos kompiuterių, mobiliųjų įrenginių, kompiuterių tinklo, programinės įrangos ir kitų informaciją (duomenis) apdorojančių informacinių technologijų priemonių (toliau – informacijos apdorojimo priemonės) valdymo ir administravimo principus;

1.2. reikalavimus teisėtam ir saugiam informacijos apdorojimo priemonių naudojimui;

1.3. prieigos prie informacijos apdorojimo priemonių ir juose esančios informacijos (toliau – Tarybos informaciniai ištekliai) suteikimo tvarką.

2. Tarybos nariai, valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis (toliau kartu – Darbuotojai), Taryboje praktiką atliekantys asmenys (toliau – praktikantai) privalo susipažinti su šiuo Aprašu ir jo laikytis.

3. Aprašas parengtas vadovaujantis:

3.1. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymu;

3.2. Kibernetinio saugumo įstatymu;

3.3. 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“;

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

3.5. 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“.

II SKYRIUS
PAGRINDINĖS SĄVOKOS

4. **Administratorius** – Tarybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, kuriam Tarybos pirmininko įsakymu yra suteikta teisė tvarkyti Tarybos informacijos apdorojimo priemones, užtikrinantis Tarybos informacijos apdorojimo priemonių veikimą ir elektroninės informacijos saugą, ar kitas asmuo (asmenų grupė), kuriam (kuriai) Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 41 straipsnyje nustatytomis sąlygomis ir tvarka perduotos informacijos apdorojimo priemonių priežiūros ir (arba) informacijos (duomenų) tvarkymo funkcijos.

5. **Kriptografinių priemonių administratorius –** Tarybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, atsakingas už kriptografinių priemonių administravimą Taryboje.

6. **Kompiuterinė įranga** – tai sisteminis blokas ar nešiojamas kompiuteris ir jo dalys, išoriniai įrenginiai (monitoriai, skaitytuvai, spausdintuvai, kopijavimo aparatai, klaviatūros, pelės,

kolonėlės, ausinės, vaizdo bei fotokameros, multimedijos projektoriai ir pan.), kompiuterių tinklo įranga, serverių, tinklo įrangos montavimo spintos, nenutrūkstamo maitinimo šaltiniai ir pan.

7. **Naudotojas** – Darbuotojas ar trečiasis asmuo, kuriam Tarybos nustatyta tvarka yra suteikiama prieiga prie Tarybos informacinių išteklių.

8. **Kompiuterių tinklas** – tai iš vieno ar daugiau kompiuterių, serverių, tinklo įrangos (kabelių, aparatinės įrangos), išorinių įrenginių, programinės įrangos ir elektroninių ryšių tinklų sudaryta ir informacinių technologijų pagrindu veikianti infrastruktūra (toliau – IT infrastruktūra), skirta užtikrinti Tarybos informacinių išteklių naudotojams operatyvų keitimąsi informacija (duomenimis).

9. **Padidinto saugumo tinklas** – tai kompiuterių tinklas, skirtas padidinto konfidencialumo informacijai, gautai iš Europos Sąjungos Energetikos reguliavimo institucijų bendradarbiavimo agentūros (angl. *European Union Agency for the Cooperation of Energy Regulators,* ACER) 2011 m. spalio 25 d. Europos Parlamento ir Tarybos reglamento (ES) Nr. 1227/2011 dėl didmeninės energijos rinkos vientisumo ir skaidrumo (toliau – REMIT) informacinės sistemos (angl. *Agency's REMIT Information System, ARIS*), išskyrus Centralizuotos Europos rinkos dalyvių registro platformos (angl. *Centralised European Registry for Energy Market Participant, CEREMP*) apdoroti.

10. **Programinė įranga** – tai programų rinkinys arba programų sistema, skirta valdyti kompiuterinę įrangą, techninę įrangą, atlikti informacijos (duomenų) apdorojimo procesus, pateikti informacijos (duomenų) apdorojimo rezultatus ir (arba) atlikti tam tikras konkrečias, tikslines, taikomąsias užduotis.

11. **Privilegijuota prieiga** – prieigos teisė arba prieigos teisių rinkinys, suteikiantis teisę Tarybos informacinių išteklių naudotojui techniniu ir (arba) programiniu lygmeniu administruoti informacijos apdorojimo priemones, t. y. atlikti administratoriaus teisių reikalaujančias funkcijas arba atlikti informacijos saugos įgaliotinio teisių reikalaujančias funkcijas.

12. **Keitimas** – bet kurios informacijos apdorojimo priemonės, IT infrastruktūros ar jos komponento pridėjimas, išėmimas ir (arba) modifikavimas.

13. **Keitimų valdymas** – procesas keitimų gyvavimo ciklui valdyti, kurio pagrindinis tikslas – atlikti pokyčius informacijos apdorojimo priemonėse, IT infrastruktūroje minimaliai trikdant Tarybos veiklą.

14. **Laikmena** – atmintinė elektroninei informacijai įrašyti. Laikmenos yra optiniai diskai (CD/DVD, angl. *Compact Disc / digital versatile disk*), USB (angl. *unversal serial bus*) sąsają turinčios laikmenos – USB atmintinės (angl. *flash drive*), išoriniai standieji diskai (angl. *hard disk drive , HDD*), įrenginiai, kuriuose atmintinės įmontuotos stacionariai ir kurių negalima išardyti, taip pat kiti objektai, skirti elektroninei informacijai įrašyti.

15. **Informacijos saugumo įvykis** – Tarybos informacijos saugumo (konfidencialumo, vientisumo ir prieinamumo) įvykiai, techninės ir (ar) programinės įrangos sutrikimai, neįprastas jų veikimas, neveikiančios arba netinkamai veikiančios fizinės apsaugos sistemos (vaizdo stebėjimo, įeigos kontrolės, signalizacijos ir pan.) ar kitos informacijos saugumo užtikrinimo priemonės, asmenų (darbuotojų ar lankytojų) veika, dėl kurios gali būti sutrikdyta Tarybos valdomų informacinių išteklių ar apsaugos sistemų veikla, pavogta, prarasta, sunaikinta, sugadinta, pasisavinta ar kitaip neteisėtai tvarkoma informacija, duomenys ar kiti informaciniai ištekliai.

16. **Informacijos saugumo incidentas** (toliau – Incidentas) – kibernetinis incidentas, elektroninės informacijos saugos incidentas arba asmens duomenų saugumo pažeidimas.

17. **Centralizuoto kompiuterių ir mobiliųjų įrenginių administravimo sistema** (toliau – Centralizuoto administravimo sistema) – tai programinė įranga, skirta centralizuotai valdyti (administruoti) Tarybos kompiuterius ir mobiliuosius įrenginius, centralizuotai atlikti tam tikras įrenginių valdymo (administravimo) užduotis (pavyzdžiui, įdiegti programinę įrangą, prisijungti prie įrenginio nuotoliniu būdu ir pan.).

18. **Atsakingas darbuotojas** – Tarybos darbuotojas, kuris vykdant pareigybės aprašyme arba Tarybos pirmininko įsakymu nustatytas funkcijas yra atsakingas už kompiuterinės įrangos ar kitų Tarybos informacijos apdorojimo priemonių išdavimą eksploatacijai ir jų apskaitą.

19. **Failų serveris** – duomenų laikymui ir dalijimuisi skirta virtuali tarnybinė stotis, kurią gali pasiekti ir vienu metu kreiptis keli kompiuterių tinklo naudotojai.

20. **Aktyvusis katalogas** (angl. *Active Directory*) – programinė įranga, skirta centralizuotai valdyti Tarybos kompiuterių tinklą, nustatyti saugumo taisykles (politiką), kurti Tarybos informacinių išteklių naudotojų paskyras, nustatyti naudotojų prieigos teises ir pan.

21. **Tretieji asmenys –** tai asmenys, nesusiję valstybės tarnybos ar darbo santykiais su Taryba.

22. **Informacijos saugos įgaliotinis** – Tarybos pirmininko įsakymu paskirtas Tarybos valstybės tarnautojas ar darbuotojas, dirbantis pagal darbo sutartį, koordinuojantis ir prižiūrintis informacijos saugumo politikos įgyvendinimą Taryboje.

23. **Mobilieji įrenginiai** – nešiojamieji kompiuteriai, judriojo ryšio telefonai, planšetės.

24. **Tiekėjas** – Tarybos informacijos apdorojimo priemonių priežiūros ir (arba) informacinių sistemų kūrimo, diegimo, priežiūros, konsultavimo, duomenų tvarkymo ar kitas paslaugas teikiantys fiziniai ar juridiniai asmenys, su kuriais Taryba yra sudariusi sutartį dėl tokių paslaugų teikimo.

III SKYRIUS
NAUDOTOJO PASKYRA

25. Kiekvienam Darbuotojui darbui su Tarybos informaciniais ištekliais sukuriama unikali naudotojo paskyra.

26. Tarybos informacinių išteklių priežiūrą atliekančių administratorių funkcijoms atlikti sukuriamos unikalios administratorių paskyros, kurios negali būti naudojamos kasdienėms Tarybos informacinių išteklių naudotojo funkcijoms atlikti.

27. Prie savo naudotojo paskyros Tarybos Darbuotojas gali prisijungti iš bet kurio Tarybos kompiuterio, prijungto prie aktyviojo katalogo (angl. *Active Directory*). Prisijungus prie paskyros iš kito Tarybos kompiuterio turi būti užtikrinama, kad kiekvienas naudotojas matys tik savo paskyros duomenis ir nematys kito naudotojo paskyroje esančių duomenų.

28. Naudotojo tapatybė nustatoma, naudojant unikalų prisijungimo vardą ir slaptažodį. Kai techninės ir programinės galimybės leidžia, gali būti naudojamos ir kitos saugios naudotojo identifikavimo priemonės.

29. Administratorių tapatumui patvirtinti turi būti naudojamos dviejų veiksnių tapatumo patvirtinimo priemonės (jeigu toks funkcionalumas palaikomas).

30. Reikalavimai prisijungimo prie Tarybos informacinių išteklių naudotojo vardui:

30.1. naudotojo vardas sudaromas iš lotynų kalbos abėcėlės raidžių ir simbolio: „.“ (toliau – taškas);

30.2. naudotojo vardą sudaro pirmoji Tarybos Darbuotojo, praktikanto arba Tiekėjo darbuotojo vardo raidė, taškas ir pavardė (pavyzdžiui, *v.pavarde*).

30.3. jeigu naujai sudaromo naudotojo vardas sutampa su jau sukurtu naudotojo vardu, prie naujai kuriamo naudotojo vardo pirmosios vardo raidės pridedama (-os) kita (-os) iš eilės einanti (-čios) vardo raidė (-s) (pavyzdžiui, *va.pavarde, var.pavarde*).

30.4. naudotojo vardą turi sudaryti ne daugiau kaip 20 simbolių. Jeigu sudarant naudotojo vardą yra viršijamas 20 simbolių skaičius, Naudotojo varde esanti pavardė nuo galūnės yra nuosekliai trumpinama iki 20 simbolių.

31. Reikalavimai naudotojo slaptažodžiui nustatyti šio Aprašo VI skyriuje.

IV SKYRIUS
KOMPIUTERIO NAUDOJIMAS

32. Kiekvienam Darbuotojui jo darbo Taryboje laikotarpiui skiriamas kompiuteris Darbuotojo darbo funkcijoms vykdyti.

33. Tarybos padidinto saugumo tinkle įdiegtų kompiuterių naudojimo reikalavimai yra nustatyti Padidinto saugumo tinkle tvarkomos informacijos naudojimo apraše.

34. Kompiuterių konfigūravimą, kompiuteryje įdiegtos programinės įrangos diegimą, keitimą, šalinimą atlieka administratorius.

35. Kiekvienas Darbuotojui skirtas kompiuteris turi būti prijungtas prie aktyviojo katalogo (angl. *Active Directory*).

36. Administratorius privalo užtikrinti, kad visuose kompiuteriuose būtų:

36.1. įdiegta Centralizuoto administravimo sistemos programinė įranga;

36.2. įdiegta centralizuotai valdoma ir atnaujinama kenksmingosios programinės įrangos aptikimo programinė įranga;

36.3. įdiegta Centralizuoto laikmenų valdymo programinė įranga, nustatanti įrenginiui leistinų naudoti USB sąsają turinčių įrenginių sąrašą, visus kitus uždraudžiant (angl. *whitelist*). Šis reikalavimas netaikomas padidinto saugumo tinkle įdiegtiems kompiuteriams.

36.4. taikoma minimali Centralizuoto administravimo saugumo politika, kuri nustatytų:

36.4.1. automatinį ekrano užrakinimą įrenginiu nesinaudojant daugiau kaip 10 min.;

36.4.2. privalomą ekrano slaptažodį, kuris turi atitikti Aprašo VI skyriuje nustatytus reikalavimus slaptažodžio ilgiui, sandarai, galiojimo trukmei;

36.4.3. duomenų šifravimą, jeigu tokia galimybė yra;

36.4.4. kompiuterio sinchronizavimąsi su Centralizuoto administravimo sistemos programine įranga ne rečiau kaip kartą per savaitę.

37. Siekiant užtikrinti kompiuterio, jame įdiegtos programinės įrangos, tvarkomos informacijos (duomenų) saugumą, naudotojams turi būti apribojamos teisės diegti programinę įrangą kompiuteriuose.

38. Darbuotojui draudžiama:

38.1. leisti naudotis kompiuteriu ir (ar) jame įdiegta programine įranga pašaliniams asmenims;

38.2. taisyti, laužyti ir gadinti kompiuterį ar kitą jam išduotą kompiuterinę įrangą;

38.3. savavališkai, be administratoriaus žinios ir leidimo, keisti Darbuotojui priskirtą kompiuterį ar kitą kompiuterinę įrangą, perkelti stacionariai įdiegtą kompiuterinę įrangą į kitą darbo vietą;

38.4. išnešti iš Tarybos patalpų kompiuterinę įrangą, išskyrus nešiojamus kompiuterius ar kitą įrangą, kai tai būtina tiesioginėms Darbuotojo darbo funkcijoms vykdyti. Šis draudimas netaikomas administratoriams, Turto valdymo ir informacinių technologijų skyriaus (toliau – TVITS) darbuotojams, kurie vykdo kompiuterinės įrangos priežiūros funkcijas;

38.5. naudoti kompiuterius ir (ar) kitą kompiuterinę įrangą veiklai, kuri nesusijusi su Darbuotojo atliekamomis funkcijomis, įskaitant (pvz., naršyti pornografiniuose, smurtą, terorizmą bei kitokią nusikalstamą veiklą propaguojančiuose tinklalapiuose, elektroniniu paštu platinti kenkėjiško pobūdžio elektroninius laiškus, failus, programas);

38.6. atlikti veiksmus, pažeidžiančius fizinio ar juridinio asmens teises, kurias saugo autorių, gretutinių ir intelektinės nuosavybės teisių apsaugos įstatymai;

38.7. vykdyti ar atidarinėti kenkėjiško kodo programas;

38.8. atskleisti prisijungimo prie kompiuterio ar kitų informacijos apdorojimo priemonių vardus, slaptažodžius arba leisti naudotis savo prisijungimo duomenimis kitiems asmenims;

38.9. atlikti bet kokio pobūdžio veiksmus, kurie trikdo kompiuterio veikimą arba gali sukelti incidentą;

38.10. savavališkai keisti suteiktus kompiuterio tinklo parametrus (pvz., IP adresą), trinti, keisti darbo metu tvarkomą, naudojamą ar sukurtą informaciją siekiant pakenkti Tarybai ar jos darbuotojams;

38.11. vykdyti failų mainus tarp interneto naudotojų naudojant lygiavertiškumo (angl. *Peer to peer*, P2P) tipo programas (pvz.: „µTorrent“, „eMule“, „DC++“, „BitComet“ ir kt.);

38.12. neturint leidimo naudotis kito Darbuotojo kompiuteriu ar kita kompiuterine įranga.

39. Kompiuterio naudotojas privalo:

39.1. kilus klausimams dėl kompiuterio ar jame įdiegtos programinės įrangos naudojimo kreiptis į administratorių;

39.2. leisti administratoriui įvertinti kompiuterio būklę;

39.3. apsaugoti kompiuterį asmeniniu slaptažodžiu Aprašo VI dalyje nustatyta tvarka;

39.4. apie informacijos saugumo įvykį ar incidentą Informacijos saugumo incidentų valdymo tvarkos aprašo nustatyta tvarka nedelsdamas pranešti informacijos saugos įgaliotiniui, administratoriui, duomenų apsaugos pareigūnui.

39.5. pasitraukdamas iš darbo vietos imtis priemonių, kad su informacija, kurią jis tvarko Tarybos informaciniuose ištekliuose, negalėtų susipažinti pašaliniai asmenys:

39.5.1. atsijungti nuo informacinių sistemų;

39.5.2. įjungti kompiuterio ekrano užsklandą, apsaugotą slaptažodžiu.

39.6. baigus darbą uždaryti visas aktyvias programas, failus, išsiregistruoti iš savo naudotojo paskyros ir išjungti kompiuterį (išskyrus atvejus, kai, siekiant nesutrikdyti veiklos procesų, jis turi būti paliktas įjungtas, bet apsaugotas ekrano slaptažodžiu).

V SKYRIUS
MOBILIŲJŲ ĮRENGINIŲ NAUDOJIMAS

40. Nešiojamų kompiuterių naudojimui taikomi Aprašo IV skyriuje nurodyti naudojimosi kompiuteriu reikalavimai, šio skyriaus reikalavimai ir žemiau nurodytos papildomos apsaugos priemonės, kurias turi užtikrinti administratorius:

40.1. prisijungimas prie nešiojamo kompiuterio operacinės ir BIOS sistemos turi būti apsaugotas slaptažodžiu;

40.2. turi būti įjungtas įrenginio duomenų šifravimas, jeigu tokia galimybė yra;

40.3. turi būti įdiegta programinė įranga skirta prisijungti prie Tarybos virtualaus privataus tinklo (angl. *Virtual private network, VPN*).

40.4. nenaudojant *WiFi* (angl. *wire-free/wireless communication, WiFi*), *„Bluetooth“* ar kitų belaidžio ryšio technologijų – jų funkcijos turi būti išjungtos.

41. Administratorius privalo užtikrinti, kad visuose Tarybos valdomuose mobiliuosiuose telefonuose ir planšetėse būtų:

41.1. įdiegta Centralizuoto administravimo sistemos programinė įranga;

41.2. įdiegta Centralizuotai valdoma ir atnaujinama kenksmingosios programinės įrangos aptikimo programinė įranga.

41.3. taikoma minimali centralizuoto administravimo saugumo politika, kuri nustatytų:

41.3.1. automatinį ekrano užrakinimą įrenginiu nesinaudojant daugiau kaip 10 minutes;

41.3.2. privalomą ekrano slaptažodžio, kuris turi būti ne trumpesnis kaip 6 simboliai ir kurį būtų privaloma keisti ne rečiau kaip kas 3 mėnesius, naudojimą;

41.3.3. įrenginio duomenų šifravimą, jeigu tokia galimybė yra;

41.3.4. privalomai įjungtus automatinius naujinimus (jei techninės galimybės leidžia tai nustatyti);

41.3.5. draudimas įrenginyje ar jo programinėje įrangoje išsaugoti slaptažodį (jei techninės galimybės leidžia tai nustatyti);

41.3.6. įrenginio sinchronizavimą su Centralizuoto administravimo sistemos programine įranga ne rečiau kaip kartą per savaitę.

42. Administratorius, naudodamasis Centralizuoto valdymo sistemos programine įranga, turi reguliariai tikrinti mobiliųjų įrenginių būklę, siekiant užtikrinti, kad:

42.1. Būtų laiku įdiegti operacinės sistemos naujinimai;

42.2. Tikrinama ar nėra įdiegta kenkimo programinė įranga;

42.3. Tikrinama, ar įrenginys atitinka minimaliuosius saugos reikalavimus.

43. Administratorius turi teisę:

43.1. Pareikalauti pristatyti mobilųjį įrenginį programinei įrangai patikrinti, atnaujinti, saugumui užtikrini.

43.2. Esant poreikiui, mobilaus įrenginio patikrinimą atlikti nuotoliniu būdu. Tokiu atveju administratorius su naudotoju suderina prisijungimo laiką. Suderintu laiku administratoriui jungiantis prie naudotojo įrenginio nuotoliniu būdu naudotojas turi patvirtinti administratoriaus prisijungimą.

43.3. Be atskiro naudotojo perspėjimo šalinti iš įrenginio kenkėjišką programinę įrangą;

43.4. Esant grėsmei mobiliosios įrangos ir (ar) informacijos (duomenų) saugumui užrakinti įrenginį arba kitaip apriboti įrangos naudotojui teises dirbti su jam priskirta įranga.

44. Mobiliųjų įrenginių naudotojas privalo:

44.1. naudotis Tarybos mobiliaisiais įrenginiais tik darbo funkcijoms vykdyti;

44.2. užtikrinti mobiliojo įrenginio fizinę apsaugą:

44.2.1. saugoti Tarybos mobilųjį įrenginį nuo aplinkos poveikio (dulkių, vibracijos, cheminių medžiagų, elektromagnetinio spinduliavimo, didelių temperatūros pokyčių);

44.2.2. nepalikti Tarybos įrenginio be priežiūros viešose vietose;

44.2.3. kelionių metu registruoti Tarybos įrenginį kaip rankinį bagažą;

44.2.4. nesinaudojant Tarybos įrenginiu, apsaugoti jį slaptažodžiu;

44.2.5. neleisti kad Tarybos įrenginiu pasinaudotų pašaliniai asmenys.

44.3. pastebėjęs įtartiną įrenginio veikimą ar galimą kenkėjišką įrangą, virusą, nedelsdamas kreiptis į administratorių;

44.4. praradus mobilųjį įrenginį ar įvykus jo vagystei, nedelsiant informuoti administratorių, Tarybos informacijos saugos įgaliotinį, Tarybos duomenų apsaugos pareigūną (apie vagystę tai pat būtina pranešti policijai bei informuoti Atsakingą asmenį);

44.5. saugoti prisijungimo duomenis (vardą ir (ar) slaptažodį), neatskleisti jų tretiesiems asmenims.

45. Darbuotojams draudžiama:

45.1. mėtyti, laužyti, daužyti, ardyti mobiliuosius įrenginius, dėti ant jų sunkius daiktus;

45.2. bandyti šalinti, apeiti ar išjungti įrenginyje nustatytus nustatymus (pavyzdžiui, atkurti mobilaus telefono gamyklinius parametrus);

45.3. ištrinti, išjungti ar kitaip apriboti Centralizuoto administravimo programinės įrangos veikimą;

46. Mobiliųjų įrenginių naudojimo reikalavimai Padidinto saugumo tinkle yra nustatyti Padidinto saugumo tinkle tvarkomos informacijos naudojimo apraše.

VI SKYRIUS
REIKALAVIMAI SLAPTAŽODŽIO SUDARYMUI, GALIOJIMO TRUKMEI, KEITIMUI IR NAUDOJIMUI

47. Reikalavimai prisijungimo prie Tarybos informacinių išteklių slaptažodžiui:

47.1. Naudotojo slaptažodį turi sudaryti ne mažiau kaip 8 simboliai;

47.2. Administratorių slaptažodį, Tarybos darbuotojų, dirbančių padidinto saugumo tinkle, slaptažodį turi sudaryti ne mažiau kaip 12 simbolių;

47.3. Slaptažodyje turi būti bent 1 (viena) raidė, bent 1 (vienas) skaičius ir bent 1 (vienas) specialusis simbolis (Administratorių slaptažodžius, Tarybos darbuotojų, dirbančių padidinto saugumo tinkle slaptažodyje turi būti bent 1 didžioji raidė, bent 1 mažoji raidė, bent 1 skaičius ir bent 1 specialusis simbolis);

47.4. Slaptažodžiams sudaryti neturi būti naudojama asmeninio pobūdžio informacija (pavyzdžiui, vardas, pavardė, gimimo data ir pan.);

47.5. Slaptažodžio sudarymui negalima naudoti klaviatūros sekos (pvz.: 123456, qwerty);

47.6. Naudotojo pirmojo prisijungimo prie Tarybos informacinių išteklių metu iš naudotojo turi būti reikalaujama, kad jis pakeistų slaptažodį;

47.7. Naudotojas, gavęs iš administratoriaus laikiną slaptažodį privalo jį pasikeisti pirmojo prisijungimo prie Tarybos informacinių išteklių metu;

47.8. Slaptažodis turi būti keičiamas ne rečiau kaip kas 3 mėnesius. Administratorių slaptažodis, Tarybos darbuotojų, dirbančių su padidinto saugumo tinkle tvarkoma informacija, slaptažodis turi būti keičiamas ne rečiau kaip kas 2 mėnesius.

47.9. Keičiant slaptažodį Tarybos aktyviojo katalogo programinė įranga neturi leisti sudaryti slaptažodžio iš buvusių 24 paskutinių slaptažodžių;

47.10. Didžiausias leistinas mėginimų įvesti teisingą slaptažodį skaičius – 5 kartai. Neteisingai įvedus slaptažodį 5 kartus, naudotojo paskyra užrakinama 15 min. Praėjus šiam terminui naudotojas gali pakartotinai mėginti įvesti slaptažodį. Dėl paskyros atrakinimo nepraėjus 15 min. terminui, naudotojas gali kreiptis į administratorių. Jeigu naudotojas pamiršo slaptažodį, dėl naujo, laikino, slaptažodžio suteikimo naudotojas turi kreiptis į administratorių. Laikinam slaptažodžiui galioja šio aprašo 47.6 – 47.7 papunkčių reikalavimai.

47.11. Didžiausias leistinas mėginimų įvesti teisingą slaptažodį jungiantis Tarybos padidinto saugumo tinkle – 3 kartai. Neteisingai įvedus slaptažodį 3 kartus, naudotojo paskyra užsirakina (užsiblokuoja) ir apie tai informuojamas administratorius;

47.12. Apie slaptažodžio galiojimo termino pabaigą naudotojas informuojamas prieš 7 dienas.

48. Naudotojai privalo saugoti slaptažodžius, neatskleisti jų tokios teisės neturintiems asmenims, o tuo atveju, jei darbuotojas slaptažodžius užsirašo, laikyti juos kitiems asmenims neprieinamose vietose (pvz., seife, rakinamame stalčiuje ir pan.) bei laikytis šių reikalavimų:

48.1. nenaudoti to paties slaptažodžio registruojantis Tarybos informaciniuose ištekliuose ir asmeninėse, su darbu nesusijusiose, paskyrose, interneto svetainėse, kompiuteriuose, mobiliuosiuose įrenginiuose ar pan.;

48.2. kilus įtarimui, kad slaptažodis yra sukompromituotas arba galėjo tapti žinomas kitiems asmenims, būtina jį pakeisti nedelsiant.

VII SKYRIUS
PRIEIGOS VALDYMAS

49. Prieigos prie Tarybos informacinių išteklių valdymas grindžiamas prielaida „viskas yra draudžiama, kas nėra aiškiai leidžiama“.

50. Prieiga suteikiama naudotojų pareigų ir vaidmenų pagrindu bei vadovaujantis:

50.1. principu „būtina naudoti“ – suteikiama prieiga tik prie informacijos apdorojimo priemonių, kurių reikia užduočiai ir (arba) darbui, ir (arba) vaidmeniui atlikti;

50.2. principu „būtina žinoti“ – suteikiama prieiga tik prie informacijos, kurios reikia užduotims atlikti (skirtingos užduotys ir (arba) funkcijos reiškia skirtingą būtinybę žinoti, taigi ir skirtingą prieigos profilį);

51. Prieigos prie Tarybos informacinių išteklių teisės turi būti suteikiamos vadovaujantis dokumentuotomis naudotojo rolėmis ir kiekvienai rolei priskirtomis teisėmis.

52. Naudotojams negali būti suteikiamos administratoriaus teisės. Privilegijuota prieiga gali būti suteikiama tik Tarybos pirmininko įsakymu.

53. Darbuotojams prieiga prie Tarybos informacinių išteklių ir teisė tvarkyti informaciją (duomenis) turi būti suteikiama tik darbuotojui nustatyta tvarka susipažinus su teisės aktais, reglamentuojančiais saugų informacijos tvarkymą Taryboje ir pasirašius Konfidencialumo pasižadėjimą, kurio forma patvirtinta Tarybos pirmininko įsakymu 2019 m. liepos 3 d. įsakymu Nr. O1E-107 „Dėl Valstybinės energetikos reguliavimo tarybos vidaus darbo tvarkos taisyklių patvirtinimo“ (toliau – Įsakymas).

54. Supažindinimo su Tarybos informacinių išteklių saugos dokumentais tvarka nustatyta:

54.1. Valstybinės energetikos reguliavimo tarybos vidaus darbo tvarkos taisyklėse (toliau – Taisyklės), patvirtintose Įsakymu;

54.2. Tarybos valdomų ir (arba) tvarkomų valstybės informacinių sistemų, registrų duomenų saugos nuostatuose;

54.3. Tarybos padidinto saugumo tinkle tvarkomos informacijos naudojimo apraše.

55. Prieiga prie Tarybos informacinių išteklių suteikiama Darbuotojo tiesioginio vadovo prašymu:

55.1. naujo Darbuotojo priėmimo atveju pildoma darbuotojo darbo priemonių poreikio forma, patvirtinta Įsakymu ir pateikiama TVITS Taisyklių nustatyta tvarka;

55.2. Darbuotojui, kuris jau yra registruotas Tarybos informacinių išteklių naudotoju elektroniniu paštu administratoriui ir informacijos saugos įgaliotiniui pateikiant šią informaciją:

55.2.1. Darbuotojo, kuriam prašoma suteikti prieigą prie Tarybos informacinių išteklių vardą, pavardę, pareigas;

55.2.2. Tarybos informacinių išteklių (jų komponento), Tarybos valdomos informacinės sistemos (jos komponento) pavadinimą nurodant prašomas roles ir (ar) teises.

56. Darbuotojo tiesioginis vadovas atsako už poreikio naudotis Tarybos informaciniais ištekliais bei prašyme suteikti prieigą, pakeisti ir (ar) papildyti nurodytų rolių ir (ar) teisių poreikio pagrįstumą.

57. Informacijos saugos įgaliotinis, gavęs prašymą dėl prieigos teisių suteikimo (jeigu prašyme yra pateikta visa reikalinga informacija) atlieka šiuos veiksmus:

57.1. įvertina prašymo pagrįstumą ir atitinkamai atlieka Aprašo 57.2–57.4 arba 60 punkte nurodytus veiksmus;

57.2. organizuoja darbuotojo supažindinimą su Tarybos informacinių išteklių saugos dokumentais (jeigu tai yra būtina);

57.3. informuoja administratorių apie darbuotojo susipažinimą su teisės aktais, reglamentuojančiais saugų informacijos tvarkymą Taryboje;

57.4. parengia atitinkamo Tarybos pirmininko įsakymo, kuriuo yra tvirtinamas Tarybos informacinių išteklių naudotojų sąrašas, pakeitimo projektą (jeigu naudotojų sąrašas tvirtinamas Tarybos pirmininko įsakymu).

58. Aprašo 57.4 papunktyje nurodytas dokumentas rengiamas kartą per 2 mėnesius.

59. Administratorius, gavęs prašymą dėl prieigos teisių suteikimo (jeigu prašyme yra pateikta visa reikalinga informacija) atlieka šiuos veiksmus:

59.1. įvertina prašymo pagrįstumą ir, gavęs iš Tarybos informacijos saugos įgaliotinio informaciją apie darbuotojo susipažinimą su teisės aktais, reglamentuojančiais saugų informacijos tvarkymą Taryboje, atitinkamai atlieka Aprašo 59.2–59.4 arba 60 punkte nurodytus veiksmus;

59.2. jei darbuotojas nebuvo įregistruotas Tarybos informacinių išteklių naudotoju, sukuria jam paskyrą, unikalų prisijungimo prie Tarybos informacinių išteklių naudotojo vardą, laikiną slaptažodį ir suteikia prašomas Tarybos informacinių išteklių naudotojo roles ir teises;

59.3. jei darbuotojas yra registruotas Tarybos informacinių išteklių naudotoju, suteikia jam papildomas prašomas Tarybos informacinių išteklių naudotojo roles ir (ar) teises;

59.4. saugiu būdu perduoda prisijungimo duomenis tiesiogiai naudotojui ir (arba) praneša naudotojui, kad prieigos teisės suteiktos (jeigu prieigos teisės suteikiamos įtraukiant naudotoją į atitinkamą grupę arba sąrašą, atpažįstant naudotoją pagal aktyviojo katalogo (angl. *Active directory*) duomenis arba naudojant kitas specialias naudotojams administruoti skirtas technines ir (ar) programines priemones).

60. Kai administratorius ir (ar) informacijos saugos įgaliotinis, išnagrinėję prašymą dėl prieigos prie Tarybos informacinių išteklių suteikimo nustato, kad jame nurodyta informacija yra netiksli, klaidinga arba prašoma nepagrįstos rolės ir (ar) teisės, kurios panaudojimas gali turėti neigiamą įtaką Tarybos informacinių išteklių veikimui arba juose esančių duomenų saugumui, jie turi teisę atsisakyti suteikti darbuotojui prašomą teisę ir (ar) rolę. Apie sprendimą atsisakyti registruoti darbuotoją Tarybos informacinių išteklių naudotoju ir (ar) suteikti jam prieigos roles ir (ar) teises bei tokio sprendimo motyvus administratorius ir (arba) informacijos saugos įgaliotinis elektroniniu paštu arba raštu informuoja darbuotojo tiesioginį vadovą.

61. Prieiga (roles ir (ar) teises) naudotis Tarybos informacijos apdorojimo priemonėmis ir (ar) dirbti su konkrečia elektronine informacija stabdoma, kai:

61.1. įstatymų nustatytais atvejais naudotojas nušalinamas nuo darbo (pareigų);

61.2. jeigu tampa žinoma, kad naudotojas dėl ligos, komandiruotės, atostogų ar kitokių pateisinamų priežasčių negali ar negalės vykdyti savo pareigų ilgiau nei 3 mėnesius;

61.3. jeigu tampa žinoma, kad administratorius dėl ligos, komandiruotės, atostogų ar kitokių pateisinamų priežasčių negali ar negalės vykdyti savo pareigų ilgiau nei 2 mėnesius;

62. Prieiga (roles ir (ar) teises) naudotis Tarybos informacijos apdorojimo priemonėmis ir (ar) dirbti su konkrečia elektronine informacija panaikinama nedelsiant, kai:

62.1. Naudotojas ar administratorius nustoja vykdyti funkcijas, kurių vykdymui jam buvo suteikta prieiga (roles ir (ar) teises) naudotis informacijos apdorojimo priemonėmis ir (ar) dirbti su konkrečia elektronine informacija;

62.2. Administratoriaus ir informacijos saugos įgaliotinio teikimu, Tarybos pirmininko sprendimu, incidento atveju, jeigu nustatoma, kad naudotojo ar administratoriaus veiksmai galėjo turėti rimtų pasekmių Tarybos informaciniams ištekliams, jų saugumui, sutrikdyti ar turėti neigiamos įtakos Tarybos veiklai.

62.3. Pasibaigia (darbo) santykiai (atleidus darbuotoją iš darbo).

63. Siekiant apsaugoti Tarybos informacinius išteklius nuo tyčinio sugadinimo, užkirsti kelią neteisėtai pasinaudoti Taryboje tvarkoma informacija, Tarybos departamentų ir skyrių vadovai turėtų apie Aprašo 61.1, 61.2, 61.3, 62.1 ir 62.3 punktuose išvardintas aplinkybes nedelsiant informuoti informacijos saugos įgaliotinį ir administratorių.

64. Tretiesiems asmenims prieiga prie Tarybos informacinių išteklių suteikiama tik tuo atveju, jeigu to nedraudžia Lietuvos Respublikos teisės aktai ir tai yra būtina Tarybos funkcijoms vykdyti bei Tarybos veiklai užtikrinti:

64.1. Teikėjams, teikiantiems Tarybai informacinių išteklių kūrimo ir (ar) diegimo ir (ar) priežiūros ir (ar) duomenų tvarkymo paslaugas;

64.2. Įstaigoms, institucijoms, gaunančioms duomenis pagal duomenų teikimo sutartis.

65. Tretiesiems asmenims prieiga prie Tarybos informaciniuose ištekliuose tvarkomų asmens duomenų tik tuo atveju, jeigu tai aiškiai leidžia Europos Sąjungos ir (arba) Lietuvos Respublikos teisės aktai, tai yra būtina Tarybos arba Tarybos asmens duomenis gaunančios institucijos ar įstaigos teisės aktuose nustatytoms funkcijoms vykdyti:

65.1. Teikėjams, teikiantiems Tarybai informacinių išteklių kūrimo ir (arba) diegimo ir (arba) priežiūros ir (arba) duomenų tvarkymo paslaugas, tik po to, kai su Teikėju pasirašoma asmens duomenų tvarkymo sutartis;

65.2. Įstaigoms, institucijoms, gaunančioms asmens duomenis pagal su jomis sudarytas asmens duomenų teikimo sutartis.

66. Tretiesiems asmenims prieiga prie Tarybos informacinių išteklių ir jose tvarkomų asmens duomenų suteikiama sutartyse su Trečiaisiais asmenimis nustatyta tvarka ir tik jų įgaliotiems darbuotojams pasirašius konfidencialumo pasižadėjimus.

67. Visi naudotojų, administratorių teisių naudotis Tarybos informaciniais ištekliais pakeitimai turi būti fiksuojami (išsaugomi) apsaugotame nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo įvykių registravimo žurnale (angl. *log file*) ir saugomi 1 (vienerius) metus nuo įrašo datos, o pasibaigus šiam terminui automatiškai ištrinami.

68. Prieiga prie patalpų, kuriuose yra įdiegti Tarybos informaciniai ištekliai suteikiama Tarybos fizinės apsaugos organizavimo aprašo, patvirtinto Tarybos pirmininko 2019 m. rugpjūčio 16 d. įsakymu Nr. O1E-142 „Dėl Valstybinės energetikos reguliavimo tarybos fizinės apsaugos aprašo patvirtinimo, patalpų zonų nustatymo, patalpų priskyrimo saugumo zonoms ir atsakingų asmenų paskyrimo“ (toliau – Tarybos fizinės apsaugos organizavimo aprašas), nustatyta tvarka.

VIII SKYRIUS
LAIKMENŲ VALDYMAS IR NAUDOJIMAS

69. Tarybos informacijos apdorojimo priemonėse, leidžiama naudoti tik Tarybos valdomas, darbuotojams darbo Taryboje laikotarpiui išduotas laikmenas.

70. Laikmenų naudojimas Tarybos padidinto saugumo tinkle yra nustatytas Padidinto saugumo tinkle tvarkomos informacijos naudojimo apraše.

71. Taryboje elektroninei informacijai saugoti yra naudojamos:

71.1. stacionarios laikmenos – stacionariai informacijos apdorojimo priemonėse (pvz., tarnybinėse stotyse, duomenų saugyklose, stacionariai įrengtose kompiuterinėse darbo vietose) įmontuotos laikmenos;

71.2. nešiojamos laikmenos – laikmenos, kurios nėra stacionariai įmontuotos į įrenginį, arba laikmenos, stacionariai įmontuotos į tokį įrenginį, kuris gali būti lengvai perneštas iš vienos vietos į kitą (pvz., nešiojamas kompiuteris).

72. Už stacionarių laikmenų administravimą ir saugumą atsako administratorius.

73. Už nešiojamų laikmenų administravimą atsako administratorius, o už saugumą atsako Tarybos darbuotojai, kuriems nešiojamos laikmenos yra patikėtos (pasirašytinai išduotos naudoti).

74. Administratorius turi užtikrinti, kad daugkartinio naudojimo nešiojamose laikmenose (pvz., USB (angl. *Universal Serial Bus),* atmintinės (angl. *flash drive*), išorinis standusis diskas (angl. *hard disk drive, HDD))* (toliau – USB laikmena) ir mobiliuosiuose įrenginiuose įdiegtose laikmenose duomenys būtų šifruojami.

75. Administratorius turi užtikrinti kad visos Taryboje naudojamos USB laikmenos būtų užregistruotos Tarybos centralizuoto laikmenų valdymo sistemoje, o kompiuteriuose ir mobiliuosiuose įrenginiuose būtų:

75.1. įdiegta programinė įranga, skirta saugiam laikmenų naudojimui ir valdymui;

75.2. įdiegta kenksmingosios programinės įrangos aptikimo programinė įranga;

75.3. uždrausta automatinė laikmenų paleistis (angl. *autorun*);

75.4. BIOS sistema apsaugota slaptažodžiu.

76. Darbuotojas prieš pradėdamas naudoti Tarybos išduotą USB laikmeną turi ją patikrinti kenksmingosios programinės įrangos aptikimo priemonėmis prijungdamas ar įdėdamas laikmeną į kompiuterį.

77. Perkeliant informaciją (duomenis) į USB laikmenas, būtina laikytis šių atsargumo priemonių:

77.1. draudžiama fiziškai atjungti USB laikmeną nuo kompiuterio, kai vyksta duomenų perkėlimo procesas (vyksta duomenų įrašymas ir (arba) nuskaitymas iš (į) USB laikmeną);

77.2. USB laikmena turi būti išimama iš kompiuterio tik įsitikinus, kad duomenų įrašymo (perkėlimo) procesas baigėsi ir laikmena gali būti saugiai išimta (angl. *safely remove hardware*) iš kompiuterio.

78. Darbuotojas asmeniškai atsako už jam patikėtos (išduotos) nešiojamos laikmenos naudojimą pagal tiesioginę paskirtį, principo „būtina žinoti“ laikymąsi ir šių reikalavimų įgyvendinimą:

78.1. draudžiama prie Tarybos informacijos apdorojimo priemonių per USB sąsają jungti bet kokias kitas (pvz., asmeninę ar iš kito asmens gautą) USB laikmeną ar įrangą;

78.2. apie bet kokį neįprastą laikmenų veikimą arba jeigu kyla įtarimų, kad darbuotojo naudojama USB laikmena sugedo ar yra fiziškai pažeista, laikmenos naudotojas privalo nedelsdamas pranešti administratoriui;

78.3. draudžiama ardyti ir pačiam taisyti laikmenas.

79. Nenaudojamas, neįprastai veikiančias arba sugedusias laikmenas Darbuotojai turi grąžinti administratoriui.

80. Laikmenos naikinamos šio Aprašo 1 priede nurodytais būdais esant vienai iš šių aplinkybių:

80.1. jeigu jose esančios informacijos neatkuriamai ištrinti negalima šio Aprašo 2 priede nurodytais būdais;

80.2. jeigu jos nereikalingos arba netinkamos toliau naudoti.

IX SKYRIUS
DARBAS NUOTOLINIU BŪDU

81. Darbuotojams, kuriems Taisyklių nustatyta tvarka yra suteikta teisė dirbti nuotoliniu būdu, nuotolinis darbas organizuojamas naudojant Tarybos išduotas darbo priemones:

81.1. nešiojamąjį arba stacionarų kompiuterį;

81.2. monitorių, klaviatūrą, pelę, kortelės skaitytuvą;

81.3. mobilųjį telefoną;

81.4. Aprašo 81.1–81.3 papunkčiuose išvardintos įrangos eksploatavimui skirtas priemones (pvz., akumuliatorių, kroviklį, SIM kortelę ir pan.).

82. Esant poreikiui naudoti kitas, neišvardintas Aprašo 81.1–81.4 papunkčiuose priemones, jų naudojimas turi būti suderintas su Tarybos administratoriumi ir informacijos saugos įgaliotiniu.

83. Jungiantis prie Tarybos informacinių išteklių naudojamas Darbuotojo nuotolinio darbo vietoje esantis interneto ryšys ir tarnybinis virtualusis privatusis tinklas (VPN).

84. Jeigu nuotolinio darbo vietoje yra naudojamas belaidžio ryšio tinklas (*WiFi*), toks tinklas turi užtikrinti bent šiuos minimalius saugumo reikalavimus (jei darbuotojas neturi galimybės įsivertinti ar belaidžio ryšio tinklas užtikrina bent minimalius saugumo reikalavimus, darbuotojas turi kreiptis į administratorių):

84.1. turi būti apsaugotas slaptažodžiu, kurį turi sudaryti bent viena didžioji raidė, bent vienas skaičius ir bent vienas specialusis simbolis;

84.2. turi būti naudojamas šifravimas WPA2 (angl. *WiFi Protected Access 2*) arba aukštesniu saugumo lygiu;

84.3. maršrutizatoriuje turi būti pakeistas standartinis, gamintojo nustatytas, slaptažodis.

85. Už nuotoliniam darbui skirtos, šio Aprašo 81.1–81.4 papunkčiuose išvardintos, įrangos fizinį saugumą atsako darbuotojas, kuriam tokia įranga pasirašytinai yra išduota.

86. Minimalūs fizinės apsaugos reikalavimai, taikomi nuotolinio darbo vietų įrengimui bei mobiliųjų įrenginių eksploatavimui laikino išvykimo iš nuolatinės ar nuotolinio darbo vietos metu yra nustatyti Tarybos fizinės apsaugos organizavimo aprašo VIII skyriuje.

87. Darbuotojas privalo:

87.1. Rūpestingai prižiūrėti ir naudoti pagal paskirtį jam išduotas, nuotoliniams darbui skirtas darbo priemones;

87.2. Saugoti nuotoliniam darbui skirtas darbo priemones nuo trečiųjų asmenų nesankcionuotos prieigos ir neteisėto naudojimosi jomis;

87.3. Laiku pranešti administratoriui apie bet kokį netinkamą nuotoliniam darbui skirtų darbo priemonių veikimą, gedimą ar pan.;

87.4. Įstatymu nustatyta tvarka atlyginti nuostolius, jeigu nuotoliniam darbui išduotos darbo priemonės buvo sugadintos ar buvo prarastos dėl Darbuotojo kaltės.

X SKYRIUS
KOMPIUTERIŲ TINKLO NAUDOJIMAS

88. Galimybė naudotis Tarybos kompiuterių tinklu ir Tarybos kompiuterių tinklo ištekliais suteikiama tik darbo Taryboje laikotarpiu.

89. Tarybos kompiuterių tinklo ištekliai skirti darbuotojo darbo funkcijoms atlikti, mokymams ir (ar) kvalifikacijai kelti.

90. Tarybos patalpose, kuriose yra sukonfigūruotas ir naudojamas belaidžio ryšio tinklas (*WiFi*), belaidžio ryšio tinklas turi atitikti šiuos minimaliuosius reikalavimus:

90.1. belaidžio ryšio tinklas, kuriame yra prieiga prie viešo interneto turi būti atskirame tinkle negu Tarybos kompiuterių tinklas;

90.2. belaidžio ryšio tinkle turi būti naudojamas šifravimas WPA2 arba aukštesniu saugumo lygiu;

90.3. Tarybos svečiams turi būti sukuriamas atskiras, atskirtas nuo Tarybos kompiuterio tinklo, belaidžio ryšio tinklas;

90.4. maršrutizatorius turi būti įrengiamas pašaliniams asmenims neprieinamose vietose,

90.5. maršrutizatoriuje turi būti pakeistas standartinis, gamintojo nustatytas, slaptažodis;

90.6. prisijungimo prie belaidžio ryšio tinklo slaptažodį turi sudaryti bent viena didžioji raidė, bent vienas skaičius ir bent vienas specialusis simbolis;

90.7. Tarybos svečiams skirtas slaptažodis negali sutapti su Darbuotojams skirtu slaptažodžiu;

90.8. Turi būti uždrausta naudoti SNMP (angl. *Simple Network Management Protocol*) protokolą;

90.9. Turi būti išjungti nenaudojami TCP (angl. *Transmission Control Protocol*) / UDP (angl. *User Datagram Protocol*) prievadai;

90.10. Turi būti uždraustas lygiarangis (angl. *peer to peer*) funkcionalumas, neleidžiantis belaidžiais įrenginiais palaikyti ryšį tarpusavyje.

91. Kompiuterių tinklo naudotojui draudžiama:

91.1. naudoti tinklo išteklius ne darbo funkcijoms vykdyti, įskaitant, bet neapsiribojant kompiuterio tinklo išteklių naudojimą komercinei veiklai, smurto, amoralaus elgesio skatinimui, įžeidžiančių pranešimų skleidimui, pornografinei, rasinei, tautinei neapykantai ar smurtą propaguojančiai, Tarybos vardą diskredituojančiai medžiagai skleisti;

91.2. tinklo išteklius naudoti programinei įrangai arba kitai informacijai, kurios diegimas, naudojimas arba platinimas prieštarautų Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatymo, 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamento (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas) (toliau – BDAR), Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo, reikalavimams arba Tarybos teisės aktų nuostatoms;

91.3. savavališkai keisti kompiuterių tinklo nustatymus, parametrus, prisijungiant apeiti bet kurį iš įdiegtų saugumo mechanizmų;

91.4. atskleisti belaidžio ryšio tinklo, skirto darbuotojams, slaptažodį tretiesiems asmenims;

91.5. savavališkai šalinti kitų darbuotojų failus;

91.6. tinklo išteklius naudoti melagingai informacijai skleisti, įžeidinėti ar priekabiauti prie kitų asmenų naudojant Tarybos kompiuterių tinklo sistemas arba siųsti tokią informaciją, pasinaudojant Tarybos vardu;

91.7. naudoti programas ar atlikti bet kokio pobūdžio veiksmus, kurie sunkina ar trikdo kompiuterių tinklo veikimą arba gali sukelti incidentą kompiuteriuose ar kompiuterių tinkle;

91.8. naudoti asmeninę kompiuterinę įrangą, jungti ją į Tarybos kompiuterių tinklą.

92. Kompiuterių tinklo naudotojas privalo:

92.1. laikytis administratoriaus nurodymų, vykdyti visus nurodymus, susijusius su kompiuterių tinklo valdymu bei saugumu;

92.2. niekam neatskleisti naudotojui suteiktus prisijungimo vardus ir slaptažodžius;

92.3. apie informacijos saugumo įvykį ar incidentą Informacijos saugumo incidentų valdymo tvarkos aprašo nustatyta tvarka nedelsdamas pranešti administratoriui, informacijos saugos įgaliotiniui, duomenų apsaugos pareigūnui.

93. Kompiuterių tinklo naudotojo teisės:

93.1. dėl kompiuterių tinklo veikimo, kompiuterių tinkle įdiegtų programų naudojimo kreiptis į administratorių;

93.2. naudotis Failų serveriu, elektroniniu paštu, internetu ir intranetu, Tarybos valdomomis ir (ar) tvarkomomis informacinėmis sistemomis, registrais vykdant Darbuotojo pareigybės aprašyme ar įsakymu nustatytas funkcijas.

XI SKYRIUS
PROGRAMINĖS ĮRANGOS VALDYMAS IR NAUDOJIMAS

94. Tarybos valdomame kompiuterių tinkle, serveriuose, kompiuteriuose, mobiliuosiuose įrenginiuose ir kituose informaciją apdorojančiose priemonėse Tarybos veiklos procesams užtikrinti turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga.

95. Visa Taryboje naudojama programinė įranga turi būti įtraukta į leistinos naudoti programinės įrangos sąrašus. Tarybos kompiuterių tinkle, kompiuteriuose ir mobiliuosiuose įrenginiuose leistinos naudoti programinės įrangos sąrašas skelbiamas Tarybos intranete. Padidinto saugumo tinkle leistinos naudoti programinės įrangos sąrašas yra tvirtinamas Tarybos pirmininko įsakymu. Informacijos saugos įgaliotinis kartu su administratoriumi ne rečiau kaip kartą per kalendorinius metus turi peržiūrėti ir, prireikus, atnaujinti leistinos naudoti programinės įrangos sąrašus.

96. Nemokamas programas, programinės įrangos demonstracines versijas, kitą laisvai platinamą programinę įrangą leidžiama naudoti jeigu yra įgyvendinamos šios sąlygos:

96.1. yra gautas laisvai platinamos programinės įrangos gamintojo ar jo įgaliotų atstovų leidimas (kai tokio pobūdžio leidimo reikalauja licencijos sąlygos);

96.2. laisvai platinama programinė įranga yra įtraukta į leistinos naudoti programinės įrangos sąrašą.

97. Tarybos padaliniai, vykdantys programinės įrangos įsigijimo procedūras, privalo užtikrinti, kad programinė įranga būtų įsigyjama iš patikimų programinės įrangos gamintojų ar jų įgaliotų programinės įrangos tiekėjų.

98. Už programinės įrangos licencijų apskaitą ir tinkamą jų priežiūrą atsako Tarybos pirmininko įsakymu paskirti atsakingi darbuotojai.

99. Programinės įrangos diegimą, šalinimą, konfigūravimą ir atnaujinimą atlieka administratoriai.

100. Programinė įranga turi būti prižiūrima ir atnaujinama, laikantis gamintojo reikalavimų ir rekomendacijų.

101. Programinė įranga turi būti testuojama naudojant atskirą testavimui skirtą aplinką.

102. Programinės įrangos naudojimas privalo atitikti Lietuvos Respublikos autorių teisių ir gretutinių teisių įstatyme ir kituose teisės aktuose bei programinės įrangos licencijose nustatytus reikalavimus.

103. Kai Tarybos Darbuotojui ar padaliniui iškyla poreikis Tarybos veiklos procesuose naudoti laisvai platinamą programinę įrangą, kuri nėra įtraukta į leistinos naudoti Taryboje programinės įrangos sąrašą, dėl tokios programinės įrangos tinkamumo (leidimo) naudoti Darbuotojas ar padalinio vadovas elektroniniu paštu turi kreiptis į administratorius ir Tarybos informacijos saugos įgaliotinį, kartu pateikiant bent šią informaciją:

103.1. programinės įrangos pavadinimą;

103.2. programinės įrangos licencijavimo sąlygas (kai taikoma);

103.3. kokiuose Tarybos veiklos procesuose ketinama naudoti laisvai platinamą programinę įrangą.

104. Administratorius ir Tarybos informacijos saugos įgaliotinis privalo įvertinti pateiktą informaciją, galimas rizikas dėl tokios programinės įrangos naudojimo, prireikus, atlikti programinės įrangos testavimą.

105. Priėmus teigiamą sprendimą dėl programinės įrangos naudojimo Informacijos saugos įgaliotinis įtraukia ją į leistinos naudoti programinės įrangos sąrašą, o administratorius įdiegia ją Darbuotojo kompiuteryje.

106. Priėmus neigiamą sprendimą apie tai elektroniniu paštu informuojamas Darbuotojas ar padalinio vadovas. Apie neleistiną Taryboje naudoti programinę įrangą gali būti informuojami ir kiti Tarybos Darbuotojai (el. paštu ar kitu būdu).

XII SKYRIUS
ELEKTRONINIO PAŠTO NAUDOJIMAS

107. Kiekvienam Darbuotojui jo darbo Taryboje laikotarpiui darbo funkcijoms vykdyti yra sukuriamas elektroninio pašto adresas (elektroninio pašto paskyra).

108. Patogesniam laiškų išsiuntimui gali būti kuriami bendri (grupiniai) elektroninio pašto adresai, pvz., bendras@vert.lt (toliau – grupinis adresas). Grupinių adresų ir atsakingų už kiekvieno grupinio adreso naudojimą Darbuotojų sąrašas yra tvirtinamas Tarybos pirmininko įsakymu.

109. Elektroninio pašto adreso sukūrimą inicijuoja Darbuotojo tiesioginis vadovas:

109.1. naujo Darbuotojo priėmimo atveju pildoma darbuotojo darbo priemonių poreikio forma, patvirtinta Įsakymu ir pateikiama TVITS Taisyklių nustatyta tvarka;

109.2. Darbuotojui, kuris jau yra registruotas Tarybos informacinių išteklių naudotoju, elektroniniu paštu administratoriui ir Informacijos saugos įgaliotiniui pateikiant šią informaciją:

109.2.1. Darbuotojo vardą, pavardę ir pareigas;

109.2.2. kokiuose Tarybos veiklos procesuose ar Darbuotojo darbo funkcijoms vykdyti būtina suteikti prieigą prie jau sukurto grupinio adreso.

110. Elektroninio pašto adresas keičiamas, panaikinamas TVITS elektroniniu paštu Taisyklių nustatyta tvarka ir terminais gavus pranešimą apie pasikeitusį Darbuotojo vardą, pavardę, atleidimą iš darbo ir pan.

111. Elektroninio pašto adresas sudaromas naudojant lotyniškas raides pagal tokią struktūrą: vardas.pavarde@vert.lt. Jei Darbuotojas turi du vardus ir (arba) dvigubą pavardę, sudarant elektroninio pašto adresą pasirenkamas jo pirmas vardas ir (arba) pirmoji dvigubos pavardės dalis. Jei naujai kuriamas Darbuotojo elektroninio pašto adresas sutampa su jau sukurtu elektroninio pašto adresu (pvz., sutampa kelių Darbuotojų vardai ir pavardės), naujai kuriamas elektroninio pašto adresas trumpinamas, t.y. sudaromas pagal tokią struktūrą: v.pavarde@vert.lt.

112. Grupinis adresas sudaromas naudojant lotyniškas raides ir laikantis šių nuostatų:

112.1. adreso unikaliojoje dalyje (prieš „@“ simbolį) pasirenkamas vienas žodis (pvz.: „pranešk“) arba žodžių junginys (pvz., „saugos įgaliotinis“);

112.2. kai pasirinktas žodžių junginys, jis turi būti atskiriamas brūkšneliu „-“ arba tašku „.“ (pvz.: saugos.igaliotinis@vert.lt);

112.3. jeigu grupinis adresas kuriamas departamentui ir (arba) skyriui turi būti naudojami trumpiniai (pvz.: knster@vert.lt).

113. Oficialus Tarybos elektroninio pašto adresas yra info@vert.lt.

114. Darbuotojai oficialiam tarpusavio bei išoriniam bendravimui turi naudoti tik Tarybos elektroninį paštą.

115. Darbuotojui nesant darbo vietoje elektroninį paštą galima pasiekti per internetinę naršyklę adresu: https://mail.office365.com – prisijungimo vardas yra darbuotojui suteiktas elektroninio pašto adresas (pvz.: vardas.pavarde@vert.lt). Slaptažodis sutampa ir yra automatiškai sinchronizuojamas su Aktyviojo katalogo paskyros slaptažodžiu.

116. Tarybos Darbuotojų darbo organizavimui, planavimui, koordinavimui yra naudojamas elektroninio pašto paskyroje įdiegtas kalendorius.

117. Tarybos Darbuotojas darbo valandomis turi ne rečiau kaip kas 30 min. peržiūrėti informaciją elektroninio pašto dėžutėje.

118. Elektroninis paštas yra ryšio priemonė, skirta Darbuotojo tiesioginėms funkcijos atlikti, ir Darbuotojai turi naudoti ją atsakingai ir teisėtais tikslais. Darbuotojai turi žinoti, kad dėl elektroninių paštu siunčiamų elektroninių laiškų Tarybos Darbuotojams ir administracijai gali kilti teisinių padarinių, jeigu:

118.1. siunčiami ar persiunčiami elektroniniai laiškai, kuriuose yra prieštaraujančių įstatymams, neatitinkančių realybės, įžeidžiančių, užgaulių, rasistinių, propaguojančių smurtą, pornografinio pobūdžio ar nepadorių vaizdinių ar teiginių;

118.2. be autoriaus sutikimo persiunčiami autorinėmis teisėmis apsaugoti kūriniai;

118.3. išsiunčiamas elektroninis laiškas, kuriame yra kenkimo programinė įranga (angl. *malicious software / code*);

118.4. siunčiamuose elektroniniuose laiškuose yra informacija, teisės aktų nustatyta tvarka pripažįstama konfidenciali, padidinto konfidencialumo informacija ar asmens duomenys.

119. Elektroninis paštas turi būti naudojamas tik Tarybos veiklos funkcijoms atlikti.

120. Elektroninio pašto naudotojai privalo:

120.1. užtikrinti, kad pašaliniai asmenys negalėtų pasinaudoti jo elektroniniu paštu (pvz., išsiųsti elektroninius laiškus);

120.2. gavus elektroninį laišką, būtina įvertinti, ar siuntėjas (žr. laukelį „*From*:“) yra žinomas ir ar buvo tikimasi iš tokio siuntėjo gauti elektroninį laišką, o taip pat ar elektroninio laiško tema nekelia įtarimo. Jeigu elektroninio pašto naudotojui nėra žinomas elektroninio laiško siuntėjas, jo elektroniniu laišku atsiųstas failas ar nuorodos, esančios laiške kelia įtarimų, jo neatidaryti, nespausti nuorodų (angl. *hyperlink*), nepaleisti programų, neatidarinėti failų, o nedelsiant kreiptis į administratorių, Informacijos saugos įgaliotinį bei pranešti apie tokį laišką Incidentų valdymo aprašo nustatyta tvarka;

120.3. rašydamas elektroninius laiškus laikytis žemiau išvardintų nuostatų:

120.3.1. į naujai rengiamo elektroninio laiško eilutę „*To*“ turi būti įrašomi elektroninio pašto adresai tik tų asmenų, kuriems elektroninis laiškas tiesiogiai skirtas, o į eilutę „*Cc*“ įrašomi elektroninio pašto adresai tų asmenų, kuriems su elektroninio laiško turiniu reikia tik susipažinti. Siunčiant grupei asmenų, siekiant užtikrinti, kad kažkuris adresatas gautų laišką, bet jo (adresato) nematytų kiti laiško gavėjai, adresą reikia įrašyti į eilutę „*Bcc*“;

120.3.2. lauke „*Subject:"* turi būti vienu ar keliais žodžiais apibūdinama siunčiamo elektroninio laiško tema;

120.3.3. elektroninis laiškas turi prasidėti trumpu mandagiu pasisveikinimu, o laiško turinys turi būti rengiamas suprantamai ir etiškai formuluojant laiško tekstą;

120.3.4. atsakant į elektroninį laišką, rekomenduojama palikti pirminio laiško (pranešimo) tekstą;

120.3.5. kiekvienas elektroninis laiškas turi būti pasirašomas, nurodant Tarybos Darbuotojo, siunčiančio elektroninį laišką, vardą, pavardę, pareigų pavadinimą, darbovietės adresą, darbo telefono numerį, tarnybinio mobiliojo telefono numerį, elektroninio pašto adresą.

120.4. siųsdamas elektroninį laišką, visada atidžiai patikrinti užrašytą elektroninio pašto adresą, kad perduodama informacija per klaidą nebūtų nusiųsta kitam adresatui;

120.5. elektroninio laiško priede siunčiant specialių kategorijų asmens duomenis ar padidinto konfidencialumo informaciją, naudoti Tarybos elektroninio pašto aplinkoje centralizuotai įdiegtas elektroninio pašto ir (arba) siunčiamų failų šifravimui skirtas priemones arba kitas, Tarybos kriptografinių priemonių administratoriaus rekomenduojamas, kriptografines priemones (pvz., dokumentų šifravimui skirtus viešuosius ir privačiuosius raktus). Siųsti specialių kategorijų asmens duomenis ir padidinto konfidencialumo informaciją elektroninio laiško turinyje – draudžiama;

120.6. prieš išvykstant atostogauti arba į tarnybinę komandiruotę, aktyvuoti automatinio atsakymo siuntimo nustatymą, kuriame turėtų būti nurodoma bent tokia informacija:

120.6.1. kad Darbuotojas dėl atostogų, komandiruotės ar pan. neturės galimybės atsakyti į gautus elektroninius laiškus;

120.6.2. laikotarpį, kuriuo metu Darbuotojas neturės galimybės atsakyti į elektroninius laiškus;

120.6.3. Tarybos valstybės tarnautojo ar darbuotojo, kuriam bus pavesta laikinai vykdyti Darbuotojo funkcijas, vardą, pavardę, pareigas, tel. Nr. ir elektroninio pašto adresą.

121. Elektroninio pašto naudotojams draudžiama:

121.1. atidarinėti elektroninių laiškų priedus, kurie gauti iš nepatikimų siuntėjų ar atrodo įtartini;

121.2. siųsti elektroniniu paštu neužšifruotą padidinto konfidencialumo informaciją ir specialių kategorijų asmens duomenis;

121.3. siųsti elektroniniu paštu informaciją apie Tarybos informacijos saugumo užtikrinimo priemones, slaptažodžius;

121.4. nesant BDAR 6 straipsnio 1 dalyje nustatytos teisėto tvarkymo sąlygos, siųsti asmens duomenis ir (arba) nesant BDAR 9 straipsnio 2 dalyje nustatytų specialių kategorijų asmens duomenų tvarkymo sąlygų;

121.5. siųsti neteisėto turinio informaciją, įvardintą Baudžiamojo kodekso 170 str. bei Visuomenės informavimo įstatymo 19 str.;

121.6. siųsti informaciją, kuri pažeistų Autorių teisių ir gretutinių teisių įstatymo nuostatas;

121.6 siųsti elektroninius apgaulės laiškus, įspėjančius apie netikrus pavojus, bei nepageidaujamus elektroninius laiškus dideliam elektroninio pašto naudotojų skaičiui ir elektroninius laiškus, kviečiančius platinti komercinę, reklaminę ar panašaus pobūdžio informaciją,

121.7. vidaus ir išorės adresatams siųsti menkaverčio turinio elektroninius laiškus, įskaitant (bet neapsiribojant) nepageidaujamo turinio elektroninius laiškus ar klaidinančią, žeidžiančią informaciją (angl. *abusive content, spam*);

121.8. naudoti Tarybos elektroninį paštą asmeniniais tikslais (pvz., nurodyti (pateikti) Tarybos elektroninio pašto adresą asmeninių pažinčių svetainėse, elektroninėse parduotuvėse, komercinių pasiūlymų, nuolaidų, akcijų svetainėse ir pan., įsigyjant prekes arba nuolaidų korteles, laisvalaikio ir kitose su darbo funkcijomis nesusijusiose svetainėse – forumų, turizmo agentūrų, socialinių tinklų svetainėse, su išorės gavėjais susirašinėti asmeniniais klausimais ir tikslais).

122. Prieiti prie Tarybos darbuotojo elektroninio pašto paskyroje esančios informacijos, saugomos Tarybos elektroninio pašto sistemoje, gali tik pats Tarybos darbuotojas ir administratorius, atlikdamas administravimo darbus (pvz., perkeliant paskyros informaciją į kitą Tarybos darbuotojui darbo tikslais suteiktą kompiuterį) arba, kai jo to paprašo pats Tarybos darbuotojas (pvz., informacijos atstatymo ar kitokios pagalbos tikslu).

123. Tarybos darbuotojui dėl sunkios ligos, mirties, nelaimingo atsitikimo ar kitokių pateisinamų priežasčių, negalint vykdyti savo pareigų ir persiųsti Tarybos veiklos vykdymo tęstinumui užtikrinti būtiną, jo elektroninio pašto paskyroje esančią, informaciją, taip pat Tarybos darbuotojui neatvykus į darbą dėl Tarybai nežinomos priežasties, ir esant poreikiui užtikrinti Tarybos veiklos tęstinumą, tokio darbuotojo tiesioginio vadovo prašymu, Tarybos pirmininko pritarimu (užrašant rezoliuciją ant prašymo) arba Tarybos pirmininko įsakymu, kitam Tarybos darbuotojui gali būti suteikiama prieiga prie negalinčio vykdyti savo pareigų darbuotojo elektroninio pašto. Tokią prieigą suteikia Tarybos administratorius.

124. Tarybos darbuotojas, šio Aprašo nustatyta tvarka gavęs prieigą prie kito Tarybos darbuotojo elektroninio pašto adreso, privalo susipažinti tik su ta informacija, dėl kurios naudojimo jam yra suteikta prieiga, saugoti informacijos ir asmens duomenų paslaptį.

125. Administratoriai, atlikdami elektroninio pašto administravimo darbus ar spręsdami neatidėliotinas su elektroniniu paštu susijusias Tarybos IT infrastruktūros, techninės ir (ar) programinės įrangos darbo problemas, turi teisę laikinai sustabdyti Tarybos elektroninio pašto darbą, apie tai iš anksto informavę Tarybos darbuotojus elektroniniu paštu išsiunčiant informacinį pranešimą Darbuotojams.

XIII SKYRIUS
TARYBOS INTERNETO SVETAINĖS NAUDOJIMAS

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

127. Tarybos interneto svetainės ir jos tarnybinės stoties techninę priežiūrą atlieka TVITS.

128. Tarybos Veiklos valdymo skyrius (toliau – VVS) administruoja Tarybos interneto svetainėje skelbiamą informaciją.

129. Už informacijos, talpinamos į Tarybos interneto svetainę turinį (aktualumą) atsako Tarybos departamento ir (arba) skyriaus, kurio kompetencijai priklauso atitinkamos informacijos (įskaitant teisės aktus ir jų projektus) rengimas, atnaujinimas ir pateikimas, paskirti atsakingi darbuotojai. Tarybos departamentų direktoriai, skyrių vedėjai apie paskirtus atsakingus Darbuotojus turi informuoti VVS.

130. Draudžiama Tarybos interneto svetainėje skelbti asmens duomenis, kurių skelbimas nenumatytas teisės aktuose. Asmens duomenų skelbimas ir (arba) rinkimas (pvz., organizuojant apklausas ir pan.) turi būti derinamas su Tarybos duomenų apsaugos pareigūnu.

131. Siekiant apsisaugoti nuo nepageidaujamų elektroninių laiškų, Tarybos darbuotojų elektroninio pašto adresai interneto svetainėje www.vert.lt turi būti nurodomi taip, kad jų neatpažintų automatizuotos elektroninio pašto adresų paieškos priemonės.

XIV SKYRIUS
FAILŲ SERVERIO NAUDOJIMAS

132. Tarybos Failų serveris yra suskirstytas į aplankus (angl. *Folder*) pagal Tarybos struktūrinius padalinius.

133. Kiekvienas Tarybos struktūrinis padalinys turi:

133.1. aplanką, į kurį kiekvienas to padalinio darbuotojas turi teisę (rolę) „rašyti“ ir „skaityti“ informaciją, o kiti Tarybos darbuotojai tik teisę (rolę) „skaityti“ informaciją. Aplanko pavadinimas sudaromas sutrumpinant struktūrinio padalinio pavadinimą abreviatūros sudarymo principu (pvz., VVS – Veiklos valdymo skyrius, DED – Dujų ir elektros departamentas).

133.2. ribotos prieigos aplanką (pvz., VVS Private). Teisę (rolę) „rašyti“ ir „skaityti“ informaciją į ribotos prieigos aplanką suteikiama tik konkretaus padalinio darbuotojui arba darbuotojų grupei. Kitiems Tarybos Darbuotojams teisė (rolė) „rašyti“ ir „skaityti“ informaciją į ribotos prieigos aplanką nesuteikiama.

XV SKYRIUS
KOMPIUTERIŲ IR MOBILIŲJŲ ĮRENGINIŲ VALDYMAS

134.Tarybos kompiuteriai ir mobilieji įrenginiai valdomi naudojant Centralizuoto valdymo sistemą, kurią sudaro:

134.1. inventorizavimo priemonė, skirta inventorizuoti ir valdyti kompiuterinę ir mobiliąją įrangą, jos sąranką (konfigūraciją), kurti ir teikti ataskaitas;

134.2. programinės įrangos diegimo priemonė, skirta valdyti (diegti, šalinti, atnaujinti, konfigūruoti) kompiuterinę ir mobiliąją įrangą (sisteminę ir programinę);

134.3. nuotolinio valdymo priemonė, skirta patikimai ir saugiai valdyti kompiuterinę ir mobiliąją įrangą nuotoliniu būdu;

134.4. duomenų atsarginio kopijavimo priemonė, skirta kompiuterinėje ir mobilioje įrangoje esančių duomenų ir informacijos atsarginių kopijų darymui.

135. Centralizuoto valdymo sistemos struktūrą sudaro:

135.1. duomenų bazės serveris, skirtas kaupti ir saugoti informaciją apie kompiuterių ir mobiliųjų įrenginių valdymo sistemos infrastruktūrą ir kompiuterių ir mobiliųjų įrenginių konfigūraciją;

135.2. paskirstymo serveriai, skirti valdyti kompiuterių ir mobiliųjų įrenginių valdymo sistemos agentus;

135.3. valdantysis serveris, skirtas valdyti duomenų bazės serverį, paskirstymo serverius ir kompiuterių ir mobiliųjų įrenginių valdymo sistemos agentus.

136. Saugiam kompiuterių ir tarnybinių stočių darbui užtikrinti Tarybos virtualiame serveryje MultiSRV įdiegta WSUS (angl. Windows Server Update Services) tarnyba, skirta gauti aktualius atnaujinimus iš gamintojo portalo ir įdiegti juos kompiuteriuose ir tarnybinėse stotyse

137. Per WSUS atnaujinimai kompiuterinėje įrangoje diegiami automatiškai (ne rečiau kaip kartą per savaitę) iš anksto nustatytu laiku. Naudotojai įspėjami apie atnaujinimus automatizuotu būdu (pranešimu) ir, esant poreikiui gali pakeisti numatytąjį atnaujinimo paleidimo laiką, t.y. nustatyti naują atnaujinimo įdiegimo laiką nei standartinis nustatytasis laikas. Įdiegus atnaujinimus naudotojui gali prireikėti paleisti kompiuterį iš naujo. Apie tai naudotojas informuojamas automatizuotu pranešimu.

138. Centralizuoto valdymo sistemos administravimą ir priežiūrą vykdo administratorius.

139. Administruodamas Centralizuoto valdymo sistemą administratorius:

139.1. vykdo kompiuterių ir mobiliųjų įrenginių valdymo sistemos programinės įrangos ir jos atnaujinimų įdiegimą valdančiajame serveryje, duomenų bazės serveryje, paskirstymo serveriuose, kompiuterinėje bei mobiliojoje įrangoje;

139.2. kuria, modifikuoja ir registruoja užduotis Centralizuoto valdymo sistemos programinėje įrangoje;

139.3. analizuoja kompiuteriuose ir mobiliuosiuose įrenginiuose įdiegtos Centralizuoto valdymo sistemos netinkamo veikimo priežastis, prireikus pašalina netinkamai veikiančius ir įdiegia naujus programinės įrangos komponentus;

139.4. užtikrina, kad Aprašo 135.1–135.3 punktuose nurodyti serveriai vykdytų tik Centralizuoto valdymo sistemos administratoriaus komandas, o su šiuose serveriuose kaupiama informacija susipažintų tik tokią teisę turintys asmenys;

139.5. atlieka duomenų bazės serveryje kaupiamos informacijos atsarginių kopijų darymą.

140. Administruodamas kompiuterius ir mobiliuosius įrenginius administratorius:

140.1. atlieka kompiuterių ir (ar) mobiliųjų įrenginių ir juose įdiegtos Centralizuoto valdymo sistemos programinės įrangos priežiūrą;

140.2. į kompiuterinę ir (ar) mobiliąją įrangą diegia Centralizuoto valdymo sistemos programinės įrangos paketus;

140.3. kontroliuoja, kad į kompiuterinę ir mobiliąją įrangą būtų įdiegta tik legali, įtraukta į leistinos naudoti Taryboje programinės įrangos sąrašą programinė įranga;

140.4. naudotojo prašymu ir (arba) vykdydamas administratoriaus funkcijas įdiegia, pašalina operacinę sistemą, taikomąją ar kitą programinę įrangą kompiuteriniame ar mobiliajame įrenginyje nuotoliniu būdu;

140.5. pastebėjęs veiksmus, galinčius daryti įtaką Tarybos kompiuterių tinklo ar duomenų saugumui, apriboja kompiuterinės ar mobiliosios įrangos naudotojui teises dirbti su jam priskirta kompiuterine, mobiliąja ir (ar) programine įranga. Apie tokius veiksmus nedelsiant turi būti informuojamas Tarybos Informacijos saugos įgaliotinis, darbuotojo tiesioginis vadovas ir Administracijos direktorius.

XVI SKYRIUS
KENKSMINGOSIOS PROGRAMINĖS ĮRANGOS APTIKIMO PROGRAMINĖS ĮRANGOS NAUDOJIMAS

141. Tarybos tarnybinėse stotyse, kiekviename kompiuteryje, kiekviename mobiliajame įrenginyje turi būti įdiegta centralizuotai valdoma ir atnaujinama kenksmingosios programinės įrangos aptikimo programinė įranga, kuri turi atitikti bent šiuos minimaliuosius saugumo reikalavimus:

141.1. užtikrintų Tarybos kompiuterių tinkle įdiegtų įrenginių apsaugą realiu laiku;

141.2. vykdytų automatinį USB laikmenų nuskaitymą;

141.3. automatiškai vykdytų belaidžio ryšio tinklo saugumo patikrą;

141.4. užtikrintų Tarybos kompiuterių tinkle įdiegtų įrenginių apsaugą nuo:

141.4.1. kenkėjiškos programinės įrangos (*malicious software / code*);

141.4.2. šnipinėjimo programų (angl. *Spyware*);

141.4.3. sukčiavimo (angl. *Anti-Phishing*),

141.4.4. išpirkos reikalaujančių kenkėjų (angl. *ransomware*),

141.4.5. nepageidaujamų elektroninių laiškų (angl. *abusive content, spam*);

141.4.6. „Botinklio“ (angl. *Botnet*) atakų;

141.4.7. įsilaužimo (abgl. *Intrusion*);

141.4.8. teikiamų paslaugų trikdymo atakų: atkirtimo nuo paslaugos (angl. *Dos*) ir dedikuoto atkirtimo nuo paslaugos (angl. *DDoS*);

141.4.9. SQL įskverbties atakų (angl. *SQL injection*),

141.4.10. XSS (angl. *Cross-site scripting*) atakų.

141.5. Informuoti administratorių apie:

141.5.1. Tarybos kompiuterių tinkle įdiegtus įrenginius, kuriems yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas,

141.5.2. įrenginius, kuriuose kenksmingos programinės įrangos aptikimo programinė įranga netinkamai funkcionuoja arba yra išjungta.

142. Kenksmingos programinės įrangos aptikimo priemonės turi automatiškai atsinaujinti ne rečiau kaip kartą per 24 val.

143. Kenksmingos programinės įrangos aptikimo programinės įrangos administravimą vykdo administratorius.

144. Administratoriai privalo užtikrinti kad kenksmingos programinės įrangos aptikimo programinė įranga būtų įdiegta į kiekvieną tarnybinę stotį, kompiuterį ir mobilųjį įrenginį.

145. Administratoriai, pastebėję tarnybinių stočių, kompiuterių, mobiliųjų įrenginių užkrėtimą kenkimo programine įranga privalo nedelsdami tinklo valdymo ir apsaugos priemonėmis stabdyti tokio kenkimo programinės įrangos plitimą Tarybos kompiuterių tinkle, o taip pat į kitus kompiuterių tinklus ir apie tokį incidentą informuoti Tarybos informacijos saugos įgaliotinį Informacijos saugumo incidentų valdymo tvarkos aprašo nustatyta tvarka.

146. Naudotojams draudžiama:

146.1. keisti įdiegtos centralizuotai valdomos kenksmingosios programinės įrangos nustatymus;

146.2. bandyti įdiegti programinę įrangą, naršyti nepatikimuose interneto tinklalapiuose, atidarinėti iš įtartinų (aiškiai neidentifikuotų) asmenų gautus elektroninius laiškus bei atverti juose esančias failus ar spausti nuorodas.

XVII SKYRIUS
ATSAKOMYBĖ UŽ KOMPIUTERINĖS ĮRANGOS NAUDOJIMĄ

147. Kompiuterius, mobiliuosius įrenginius, laikmenas ir kitą Darbuotojui priskirtą kompiuterinę įrangą eksploatacijai pasirašytinai išduoda atsakingas asmuo.

148. Darbuotojai privalo saugiai, tinkamai ir ekonomiškai naudoti jiems išduotą įrangą.

149. Darbuotojas materialiai atsako už žalą, padarytą jo tyčiniais veiksmais, naudojant jam patikėtą kompiuterinę įranga, įstatymų nustatyta tvarka.

150. Darbuotojas, praradęs ar pametęs jam priskirtą kompiuterinę įrangą, privalo Informacijos saugumo incidentų valdymo tvarkos aprašo nustatyta tvarka, nedelsdamas apie tai informuoti administratorių, Tarybos Informacijos saugos įgaliotinį, Tarybos duomenų apsaugos pareigūną bei informuoti tiesioginį vadovą tiesiogiai (telefonu, el. paštu). Apie vagystę taip pat būtina pranešti policijai.

151. Pasibaigus darbo santykiams Darbuotojas jam priskirtą kompiuterinę įrangą privalo grąžinti atsakingam darbuotojui Taisyklių nustatyta tvarka.

XVIII SKYRIUS
TIEKĖJŲ VALDYMAS

152. Tiekėjų atranka ir vertinimas atliekamas vadovaujantis Lietuvos Respublikos viešųjų pirkimų įstatymo, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymo 42 punkto ir kitų teisės aktų reikalavimais.

153. Sutartyse su Tiekėjais, kuriems bus suteikiama prieiga prie Tarybos informacijos (duomenų) ir (ar) informaciją (duomenis) apdorojančių priemonių, turi būti įtraukti informacijos (duomenų) saugumo reikalavimai, susiję su veiklos, organizacinėmis ir techninėmis priemonėmis, įskaitant ir nuostatas dėl konfidencialumo užtikrinimo.

154. Tiekėjams prieiga prie Tarybos informacinių išteklių ir juose tvarkomos informacijos bei asmens duomenų gali būti suteikiama tik tokios apimties, kiek tai būtina sutarčiai įgyvendinti ir nedelsiant panaikinama, pasibaigus sutartiniams santykiams.

155. Tarybos darbuotojai, Tarybos pirmininko įsakymu paskirti atsakingais už sutarties vykdymą, privalo kontroliuoti ir užtikrinti, kad:

155.1. Sutarties vykdymo metu paslaugas teiktų tik Tiekėjo nurodyti specialistai (darbuotojai) ir tik pasirašę konfidencialumo pasižadėjimus;

155.2. Tiekėjo specialistai, kuriems sutarčiai vykdyti yra būtina prieiga prie Tarybos patalpų, kuriose yra įrengtų (įdiegtų) Tarybos informaciją apdorojančių priemonių, tokia prieiga būtų suteikiama Tarybos fizinės apsaugos organizavimo aprašo nustatyta tvarka.

155.3. Pasibaigus sutartiniams santykiams iš tiekėjo būtų reikalaujama grąžinti visą Tarybos turtą, jeigu toks buvo patikėtas sutarties vykdymo laikotarpiui ir (arba) gautą informaciją, įskaitant kopijas, jeigu tokia buvo patikėta (perduota) sutarties vykdymo metu.

156. Tarybos Informacijos saugos įgaliotinis, siekdamas patikrinti kaip Tarybos darbuotojai, paskirti atsakingais už sutarties vykdymą, laikosi šiame skyriuje nustatytų reikalavimų ne rečiau kaip kartą per kalendorinius metus atlieka Teikiamų paslaugų priežiūros kontrolę, kurios metu atsitiktinai pasirinkus galiojančią (vykdomą) Sutartį patikrinama kaip vykdant sutartį yra laikomasi šiame skyriuje ir sutartyje nustatytų informacijos saugumo reikalavimų.

157. Atsižvelgiant į patikrinimo rezultatus, informacijos saugos įgaliotinis gali inicijuoti Tarybos darbuotojų mokymus, imtis kitų priemonių (veiksmų), kurie padėtų sumažinti patikrinimo metu nustatytus trūkumus arba būtų išvengta pakartotino tokių trūkumų atsiradimo tikimybė, įvertinti riziką, susijusią su Tiekėjais, jų paslaugų vykdymu ir numatyti priemones rizikoms valdyti.

158. Tiekėjams, teikiantiems paslaugas, susijusias su Tarybos padidinto saugumo tinklo priežiūra taikomi papildomi reikalavimai, kurie yra nustatyti Padidinto saugumo tinkle tvarkomos informacijos naudojimo apraše.

XIX SKYRIUS
KEITIMŲ VALDYMAS

159. Tarybos IT infrastruktūros ir informaciją apdorojančių priemonių (techninių ir programinių) pakeitimų valdymas turi užtikrinti:

159.1. standartizuotos procedūros nustatymą visiems Tarybos informaciją apdorojančių priemonių (techninių ir programinių) pakeitimams valdyti, atsižvelgiant į šių pakeitimų gyvavimo ciklo etapus, konstravimą, testavimą, diegimą, tikrinimą (angl. *build, test, implement, verfy*);

159.2. pakeitimų sąnaudų bei rizikų dėl pakeitimų valdymą;

159.3. Tarybos Darbuotojų ir kitų suinteresuotų asmenų informavimą apie atliekamus pakeitimus;

159.4. IT infrastruktūros, informaciją apdorojančių priemonių konfidencialumą, vientisumą ir prieinamumą.

160. Poreikis keitimams gali iškilti dėl įvairių priežasčių, įskaitant, bet neapsiribojant, žemiau išvardintomis:

160.1. naudotojų prašymai;

160.2. Tiekėjų teikiamų paslaugų vykdymas;

160.3. struktūriniai pokyčiai Taryboje;

160.4. esamos techninės ir programinės įrangos pakeitimas;

160.5. naujos techninės ir (ar) programinės įrangos, naujo kompiuterių tinklo diegimas;

160.6. techninės ir (ar) programinės įrangos gedimai;

160.7. Tarybos IT infrastruktūros pasikeitimai.

161. Taryboje pakeitimai skirstomi į tokius tipus:

161.1. tipiniai pakeitimai – tai pasikartojantys, dažnai atliekami, apibrėžti ir nesudėtingi Tarybos IT infrastruktūros, informaciją apdorojančių priemonių pakeitimai;

161.2. reikšmingi pakeitimai – tai sudėtingi ir turintys reikšmingos įtakos Tarybos IT infrastruktūros, informaciją apdorojančių priemonių funkcionalumui pakeitimai:

161.2.1. visi operacinių sistemų, taikomųjų programų ir jų naujinimų pakeitimai;

161.2.2. keletas tarpusavyje susijusių keitimų, kurie turi (gali turėti) įtakos kitų IT infrastruktūros komponentų, informaciją apdorojančių priemonių funkcionalumui;

161.2.3. keitimas atliekamas daugelyje IT infrastruktūros elementų;

159.2.4 keitimas yra sudėtingas, jo rizika yra didelė todėl būtina numatyti priemones rizikai sumažinti.

162. skubūs pakeitimai — skubaus sprendimo priėmimo reikalaujantys reikšmingi Tarybos IT infrastruktūros pakeitimai.

163. Visus pakeitimus atlieka Administratoriai atsižvelgdami į šiuos reikalavimus:

163.1. visi reikšmingi pakeitimai turi būti derinami su Tarybos informacijos saugos įgaliotiniu siekiant įvertinti: keitimo būtinumą, galimą keitimo poveikio mastą ir rizikas;

163.2. jei keitimas gali turėti poveikį IT infrastruktūrai, informacijos apdorojimo priemonių vientisumui, konfidencialumui ir prieinamumui, toks keitimas turi būti atliekamas sudarant diegimo aprašą, kuriame turi būti numatyta (aprašyta):

163.2.1. pakeitimui įgyvendinti reikalingi resursai;

163.2.2. pakeitimui būtini darbai (užduotys) ir jiems atlikti skirtas laikas;

163.2.3. diegimo sąrankos aprašymas (diegimą sudarantys konfigūraciniai vienetai ir jų tarpusavio ryšys),

163.2.4. detalus testavimo planas;

163.2.5. detalus atsitraukimo (angl. *Back out*) planas;

163.2.6. testavimo eiga ir testavimo rezultatų įvertinimas,

163.2.7. numatomas diegimo į realią (gamybinę, eksploatuojamą) aplinką įgyvendinimas ir korektiškumo patikrinimas;

163.2.8. nustatomas IT infrastruktūros sąrankos, konfigūracijos vienetų, kuriems keitimas galėjo turėti įtakos stebėsenos laikotarpis.

164. Atlikus keitimus ir esant poreikiui rengiami arba patikslinami IT infrastruktūros, Informacinių sistemų sąrankos dokumentai.

165. Apie visus keitimus, kurie gali turėti įtakos informacinių sistemų, IT infrastruktūros, kompiuterių tinklo ar Tarybos informaciją apdorojančių priemonių darbui iš anksto, bet ne vėliau kaip prieš 1 darbo dieną iki tokio pakeitimo vykdymo, turi būti įspėjami visi Tarybos naudotojai ir suinteresuoti asmenys (pvz., Tiekėjai, Tarybos paslaugų naudotojai ir pan.).

166. Visi Tarybos IT infrastruktūros ir informaciją apdorojančių priemonių (techninių ir programinių) keitimai turi būti fiksuojami (registruojami):

166.1. Su Tarybos valdomų informacinių sistemų priežiūra susiję keitimai fiksuojami šių informacinių sistemų Pagalbos tarnybos sistemose, Informacinių sistemų saugos dokumentuose (techninės ir programinės įrangos sąrankos aprašuose).

166.2. Su Tarybos kompiuterių tinklo, kompiuterių, mobiliųjų įrenginių susiję keitimai (techniniai ir programiniai) fiksuojami Informacinių technologijų probleminių situacijų registracijos žurnale (bylos indeksas Nr. 17.7).

167. Atliekant keitimus visi Tarybos informacinių sistemų ir (ar) IT infrastruktūros pranešimai turi būti fiksuojami ir registruojami Pagalbos tarnybos sistemoje arba Informacinių technologijų probleminių situacijų registracijos žurnale;

168. atliekant programinės įrangos versijų keitimus turi būti fiksuojama bent ši informacija: keičiamos programinės įrangos pavadinimas, versija, paskutinė atnaujinimo data, informacija apie programinės įrangos, naudojamos IT infrastruktūroje vietą bei legalumo dokumentus.

169. Tarybos padidinto saugumo tinkle keitimų valdymo procedūroms taikomi papildomi reikalavimai, nustatyti Padidinto saugumo tinkle tvarkomos informacijos naudojimo apraše.

XX SKYRIUS
KRIPTOGRAFINIŲ PRIEMONIŲ NAUDOJIMAS IR VALDYMAS

170. Taryboje kriptografinės priemonės turi būti naudojamos, kai kyla rizika informacijos (duomenų) konfidencialumui, vientisumui ir prieinamumui ir kai kitos informacijos (duomenų) apsaugos priemonės yra nepakankamos jų saugumui užtikrinti. Šių priemonių naudojimą užtikrina administratorius.

171. Kriptografines priemones būtina naudoti:

171.1. kai nuotoliniu būdu prisijungiama prie Tarybos kompiuterių tinklo ar šiame tinkle įdiegtų informacijos apdorojimo priemonių (tokiu atveju turi būti naudojamas šifruojamasis duomenų perdavimo protokolas);

171.2. kai nuotoliniu būdu prisijungiama prie Tarybos informacinių sistemų (tokiu atveju turi būti naudojamas šifruojamasis duomenų perdavimo protokolas ir juo prisijungimo metu perduodami failai);

171.3. kai naudojami mobilieji įrenginiai (nešiojamieji kompiuteriai, planšetės, išmanieji telefonai ir pan.), nešiojamos informacijos laikmenos (tokiu atveju turi būti šifruojama mobiliuosiuose įrenginiuose, nešiojamose laikmenose esanti informacija (duomenys));

171.4. atsarginėse kopijose įrašytai elektroninei informacijai (duomenims) apsaugoti;

171.5. elektroniniu paštu perduodant specialių kategorijų asmens duomenis, padidinto konfidencialumo informaciją (duomenis).

172. Kriptografinius raktus kuria taikomoji programinė įranga ir kriptografinių priemonių administratorius.

173. Aprašo 3 priede pateikiamos rekomendacijos, kuriomis būtina vadovautis, pasirenkant Taryboje naudojamas kriptografines priemones.

174. Taryboje už naudojamų kriptografinių priemonių administravimą atsako Tarybos pirmininko įsakymu paskirtas kriptografinių priemonių administratorius, kuris:

174.1. organizuoja ir vykdo Taryboje naudojamų kriptografinių priemonių apskaitą;

174.2. kartu su Tarybos informacijos saugos įgaliotiniu:

174.2.1. įvertina kriptografinių priemonių poreikį, teikia siūlymus dėl elektroninės informacijos kriptografinės apsaugos;

174.2.2. dalyvauja nustatant kriptografinių priemonių administravimo ir kontrolės procedūras.

175. Už Taryboje naudojamų kriptografinių priemonių kontrolę atsako Tarybos informacijos saugumo įgaliotinis, kuris:

175.1. užtikrina Taryboje nustatytų kriptografinių priemonių administravimo ir saugumo procedūrų vykdymo kontrolę Taryboje;

175.2. kontroliuodamas kaip Taryboje įgyvendinami kriptografinės apsaugos reikalavimai, 1 kartą per kalendorinius metus atlieka patikrinimus;

175.3. instruktuoja kriptografinių priemonių administratorius kriptografinių priemonių apsaugos klausimais;

175.4. kartu su Tarybos kriptografinių priemonių administratoriumi:

175.4.1. įvertina kriptografinių priemonių poreikį, teikia siūlymus dėl elektroninės informacijos kriptografinės apsaugos;

175.4.2. nustato kriptografinių priemonių administravimo ir kontrolės procedūras.

176. Visos Taryboje naudojamos kriptografinės priemonės (įrenginiai, USB atmintinės, lustinės kortelės) privalo būti įtrauktos į Kriptografinių priemonių apskaitos žurnalą (Aprašo 4 priedas);

177. Tarybos darbuotojui Kriptografinės priemonės išduodamos tik jam pasirašius Kriptografinių priemonių apskaitos žurnale (Aprašo 4 priedas);

178. Kriptografinių priemonių administratorius išduodamas kriptografinius raktus ir (ar) sertifikatus privalo:

178.1. padaryti (išsaugoti) atsarginę išduodamo kriptografinio rakto ir (ar) sertifikato kopiją kriptografinių raktų ir (ar) sertifikatų archyve.

178.2. padaryti (išsaugoti) išduodamo kriptografinio rakto ir (ar) slaptažodžio kopiją.

179. Kriptografinio rakto atsarginiai slaptažodžiai turi būti saugomi pas kriptografinių priemonių administratorių atskirai nuo kriptografinių raktų.

180. Jeigu nėra galimybių naudoti programinių priemonių saugiam atsarginių slaptažodžių ir (ar) slaptos frazės saugojimui, kriptografinių priemonių administratorius turi naudoti bent tokią atsarginių slaptažodžių ir (ar) slaptos frazės saugojimo procedūrą:

180.1. slaptažodis ir (ar) frazė užrašomas ir įdedamas į voką, kuris yra užklijuojamas, antspauduojamas apsaugine užklija, kurios negalima būtų atplėšti nepažeidus voko, pasirašo arba uždeda savo spaudą ant užklijos, o ant voko nurodoma:

180.1.1. kriptografinio rakto, kuriam naudojamas slaptažodis pavadinimas;

180.1.2. asmens, kuriam kriptografinis raktas išduotas vardas, pavardė ir pareigos.

181. Už Tarybos kompiuteriniame tinkle įdiegtos kriptografines priemones (įrenginio) fizinę apsaugą atsako Tarybos kriptografinių priemonių administratorius.

182. Už Darbuotojui išduotos nešiojamos laikmenos su kriptografine priemone (įrenginio) fizinį saugumą (pvz., apsaugą nuo aplinkos poveikio, vagystės ar pan.) atsako Darbuotojas.

183. Testavimui skirtos kriptografinės priemonės neturi būti naudojamos realioje (gamybinėje) aplinkoje, o realioje (gamybinėje) aplinkoje neturi būti naudojamos kriptografinės priemonės, naudojamos testinėje aplinkoje.

184. Pasibaigus Darbuotojo darbo santykiams visos jam išduotos kriptografinės priemonės gražinamos Kriptografinių priemonių administratoriui, jam pažymint Kriptografinės priemonės gražinimo faktą Kriptografinių priemonių apskaitos žurnalą (Aprašo 4 priedas).

185. Tarybos padidinto saugumo tinkle įdiegtų kriptografinių priemonių naudojimo reikalavimai yra nustatyti Padidinto saugumo tinkle tvarkomos informacijos naudojimo apraše.

XXI SKYRIUS
INFORMACIJOS APDOROJIMO PRIEMONIŲ, INFORMACINIŲ TECHNOLOGIJŲ INFRASTRUKTŪROS, JOS NAUDOTOJŲ IR ADMINISTRATORIŲ ATLIEKAMŲ VEIKSMŲ AUDITAS IR KONTROLĖ

186. Taryboje informacijos apdorojimo priemonių, IT infrastruktūros, jos naudotojų ir administratoriaus veiksmų (toliau – įvykių) auditas ir kontrolė vykdomi naudojant įvykių registravimo žurnalus (angl. *log files*), siekiant:

184.1. nustatyti (atsekti) neteisėtus ir (ar) neleistinus naudotojų, Administratorių veiksmus, atliekamus naudojant Tarybos informacijos apdorojimo priemones, IT infrastruktūrą (pvz., įvykus incidentui, kai būtina ištirti jo atsiradimo priežastis);

184.2. fiksuoti potencialius vidinius arba išorinius bandymus pažeisti Tarybos informacijos apdorojimo priemonių, IT infrastruktūros saugumą;

184.3. fiksuoti Tarybos informacijos apdorojimo priemonių, IT infrastruktūros gedimus, techninės ir programinės įrangos klaidų pranešimus.

187. Įvykių auditui ir kontrolei atlikti įvykių registravimo žurnaluose turi būti fiksuojama ši informacija:

187.1. Tarybos informacijos apdorojimo priemonių, IT infrastruktūros elementų įjungimas, išjungimas ar perkrovimas;

187.2. Tarybos informacijos apdorojimo priemonių, IT infrastruktūros naudotojų, administratoriaus prisijungimas (ir nesėkmingi bandymai prisijungti) / atsijungimas;

187.3. Tarybos informacijos apdorojimo priemonių, IT infrastruktūros naudotojų, administratorių teisių naudotis informacinės sistemos, kompiuterinio tinklo ištekliais pakeitimai (ten, kur palaikomas toks funkcionalumas);

187.4. Audito funkcijos įjungimas, išjungimas,

187.5. Audito įrašų trynimas, kūrimas, keitimas;

187.6. Laiko ir (ar) datos pakeitimas;

187.7. Naudotojų ir administratorių Tarybos informacinėse sistemose ir informaciniuose ištekliuose atliekami veiksmai (pvz., duomenų įvedimas, peržiūra, keitimas, panaikinimas), naudotojų ir administratorių teisių pakeitimai, papildymai, panaikinimai;

187.8. tinklo įrangos įvykiai;

187.9. Programinės įrangos, įskaitant skirtos apsaugai nuo kenksmingos Programinės įrangos, įvykiai;

187.10. IT infrastruktūros parametrų pasikeitimai;

187.11. bandymai vykdyti kibernetines atakas.

188. Audituojamų įrašų laiko žymos turi būti sinchronizuotos ne mažiau kaip 1 sekundės tikslumu ir turi būti naudojami mažiausiai 2 laiko sinchronizavimo šaltiniai.

189. Kiekviename audito duomenų įraše turi būti fiksuojama:

189.1. įvykio data ir tikslus laikas;

189.2. įvykio rūšis/pobūdis;

189.3. įvykio trukmė;

189.4. įvykio rezultatas;

189.5. naudotojo, Administratoriaus ir (arba) įrenginio, susijusio su įvykiu duomenys (identifikatoriai).

190. Įvykių registravimo žurnaluose duomenys saugomi 1 metus nuo įrašo datos, o pasibaigus šiam terminui automatiškai sunaikinami;

191. Įvykių registravimo žurnalų duomenys turi būti saugomi kitoje vietoje, t.y. ne tame pačiame įrenginyje ar informacinėje sistemoje, kurio (-ios) įvykių registravimo žurnalų duomenys buvo surinkti.

192. Įvykių registravimo žurnalai turi būti apsaugoti nuo klastojimo ir neteisėtos prieigos prie jų. Turi būti neįmanoma juos ištrinti ar pakeisti jų turinį.

193. Prieiga prie įvykių registravimo žurnalų turi būti registruojama.

194. Įvykių registravimo žurnalų analizę atlieka administratorius, ne rečiau kaip kartą per savaitę.

XXII SKYRIUS
KOMPIUTERINĖS (TECHNINĖS IR PROGRAMINĖS) ĮRANGOS APSKAITA, TAISYMAS, NURAŠYMAS, NAIKINIMAS IR PAKARTOTINIS NAUDOJIMAS

195. Visa Tarybos įsigyta kompiuterinė (techninė ir programinė) įranga turi būti įtraukiama į Tarybos įsigyto nematerialaus arba ilgalaikio ir trumpalaikio materialaus turto (toliau – Turtas) apskaitą.

196. Turto apskaita, išdavimas (perdavimas) eksploatacijai, grąžinimas ir nurašymas vykdomas Tarybos turto tvarkymo taisyklių, patvirtintų Tarybos pirmininko 2019 m. lapkričio 11 d. įsakymu Nr. O1E-190 „Dėl Valstybinės energetikos reguliavimo tarybos turto tvarkymo taisyklių“ (toliau – Įsakymas) nustatyta tvarka.

197. Turto apskaitą, išdavimą (perdavimą) eksploatacijai ir nurašymą vykdo atsakingi asmenys, paskirti Įsakymu.

198. Už eksploatacijai išduoto turto saugumą atsako Turtą eksploatuojantys asmenys:

198.1. Darbuotojai – už pasirašytinai jiems išduotus kompiuterius, mobiliuosius įrenginius, nešiojamas laikmenas, programinę įrangą ir kitą kompiuterinę įrangą;

198.2. Administratoriai – už Tarybos komutacinėse patalpose įdiegtą, Tarybos informacinėse sistemose, kompiuteriniuose tinkluose įdiegtą techninę, programinę įrangą, stacionarias laikmenas.

199. Sugedusį Turtą Darbuotojai turi grąžinti atsakingam asmeniui, kuris, priklausomai nuo Turto būklės, organizuoja Turto taisymą arba nurašymą Tarybos turto tvarkymo taisyklių nustatyta tvarka ir laikydamasis šių reikalavimų:

199.1. taisymui sugedusi techninė įrangą gali būti atiduodama tik išėmus atmintinės, diskus, kuriose gali būti Tarybai svarbios informacijos;

199.2. padidinto konfidencialumo informacijos apdorojimo tinkle įdiegtos įrangos remontas vykdomas tik Tarybos patalpose ir tik dalyvaujant šio tinklo Tarybos administratoriui.

200. Laikmenos naikinamos šio Aprašo 1 priede nurodytais būdais.

201. Pakartotinai naudoti techninę įrangą galima tik atlikus šioje įrangoje buvusių laikmenų neatkuriamą trynimą šio Aprašo 2 priede nurodytais būdais arba, kai laikmenos techninėje įrangoje buvo pakeistos naujomis.

XXIII SKYRIUS
ATSARGINIŲ ELEKTRONINĖS INFORMACIJOS KOPIJŲ DARYMO IR NAUDOJIMO REIKALAVIMAI

202. Už reguliarų elektroninės informacijos atsarginių kopijų (toliau – atsarginės duomenų kopijos) darymą, užtikrinimą, kad jos būtų daromos Tarybos informacijos apdorojimo priemonių, IT infrastruktūros priežiūros dokumentuose bei Tarybos valdomų informacinių sistemų duomenų saugos nuostatuose nustatyta tvarka, numatytu laiku (periodiškumu) ir numatyta apimtimi atsako administratorius.

203. Atsarginės duomenų kopijos daromos automatiniu būdu į specialiai tam skirtas duomenų saugyklas, serverius, o kai tokios galimybės dėl techninių ar kitų priežasčių nėra – rankiniu būdu į išorines laikmenas (pvz., standžiuosius diskus).

204. Prieš atliekant bet kokį Tarybos informacijos apdorojimo priemonių, IT infrastruktūros ar Tarybos valdomų informacinių sistemų pakeitimą turi būti daromos atsarginės duomenų kopijos:

205. techninės ir (arba) programinės įrangos konfigūracijos nustatymų (kai pakeitimai susiję su šios įrangos konfigūracijos nustatymų keitimu ar pan.);

206. informacinių sistemų duomenų bazių (kai pakeitimai gali turėti įtakos duomenų bazėse saugomų duomenų saugumui (vientisumui, konfidencialumui, prieinamumui)).

207. Elektroninė informacija atsarginėse duomenų kopijose turi būti laikoma užšifruota, o jeigu tokios galimybės nėra, turi būti taikomos kitos apsaugos priemones, apsaugančios nuo nesankcionuoto priėjimo prie atsarginių duomenų kopijų, jų panaudojimo ar sunaikinimo (pvz., seifai);

208. Atsarginės duomenų kopijos turi būti fiziškai saugomos atskirai nuo realių duomenų (pvz., kriptografinėmis priemonėmis apsaugotame įrenginyje, kitose patalpose ir (arba) kitame pastate nei yra įrenginys, kurio elektroninė informacija buvo nukopijuota).

209. Tarybos valdomų informacinių sistemų tarnybinių stočių programinės įrangos atsarginės duomenų kopijos turi būti laikomos kitose patalpose arba kitame pastate nei yra tarnybinės stotys, kurių programinė įranga buvo nukopijuota.

210. Fizinė prieiga prie techninės įrangos, laikmenų, seifų, patalpų, kuriose yra saugomos atsarginių duomenų kopijos, suteikiama tik administratoriams.

211. Taryboje daromos šių tipų atsarginių duomenų kopijos:

212. pilna kopija (angl. *full backup*) – atsarginė kopija, kurioje saugomi visi pažymėtų failų duomenys nuo atitinkamo laiko;

213. prieauginė kopija (angl. *Incremental backup*) – atsarginė kopija, kurioje saugomi tik tie failų pakeitimai, kurie buvo padaryti po paskutinės pilnos kopijos (išsaugomi nuo padarytos pilnos kopijos pakitę duomenys);

214. realaus laiko atsarginė kopija (angl. *hot backup*) – atsarginė kopija, kuri daroma realiuoju laiku, nepertraukiant informaciją apdorojančios įrangos, IT infrastruktūros ar informacinės sistemos darbo.

215. Kiekvienas atsarginės duomenų kopijos padarymas ir visi veiksmai, atliekami su atsarginių duomenų kopijomis turi būti fiksuojami įvykių registravimo žurnaluose (angl. *log files*).

216. Atsarginės duomenų kopijos naudojamos:

216.1. atkurti informacijos apdorojimo priemonių, IT infrastruktūroje įdiegtos techninės ir (ar) programinės įrangos, informacinių sistemų funkcionalumą, įskaitant, bet neapsiribojant informacijos (duomenų) atkūrimą;

216.2. atliekant incidento tyrimą (išimtinai tik incidento priežasčiai ir aplinkybėms nustatyti);

216.3. atliekant informacinių sistemų tęstinumo valdymo planuose numatytus testavimus.

217. Aprašo 216 punkte nurodytais atvejais atsarginės duomenų kopijos naudojamos tik jeigu toks jų panaudojimas yra fiksuojamas (registruojamas) (pvz., Pagalbos tarnyboje arba Informacinių technologijų probleminių situacijų registracijos žurnale (bylos indeksas Nr. 17.7)).

218. Administratorius privalo:

219. laikytis Taryboje nustatytos atsarginių duomenų kopijų darymo tvarkos;

220. kartą per savaitę peržiūrėti atsarginių duomenų kopijų fiksavimo įvykių registravimo žurnalus (angl. *log files*);

221. kartą per kalendorinius metus testuoti duomenų atstatymą iš atsarginių duomenų kopijų;

222. tikrinti duomenų vientisumą, atliekant duomenų atstatymo testavimą;

223. Atsarginės duomenų kopijos saugomos 1 kalendorinius metus nuo paskutinės atsarginės kopijos įrašymo dienos, jeigu Tarybos valdomų informacinių sistemų duomenų saugos nuostatuose nenumatyta kitaip.

224. Elektroninio pašto, elektroninių laiškų atsarginės duomenų kopijos, elektroninio pašto atsarginių kopijų saugojimo programinėje įrangoje saugomos 1 kalendorinius metus nuo elektroninio laiško gavimo datos.

225. Laikmenos, kuriose yra saugomos atsarginės duomenų kopijos, pasibaigus kopijų saugojimo terminui gali būti naudojamos naujoms atsarginių duomenų kopijoms daryti, o netinkamos laikmenos turi būti sunaikinamos šio Aprašo 1 priede nustatytais būdais.

XXIV SKYRIUS
BAIGIAMOSIOS NUOSTATOS

226. Informacijos saugos įgaliotinis kasmet organizuoja Darbuotojų mokymus dėl Aprašo reikalavimų ir (ar) kitais informacijos saugos klausimais, nuolat jiems primena informacijos saugos reikalavimus (elektroniniu paštu, atmintinėmis ir pan.).

227. Darbuotojai, pažeidę šio Aprašo nuostatas atsako Lietuvos Respublikos įstatymų ir kitų teisės aktų nustatyta tvarka.

228. Visi kiti šiame Apraše nenumatyti Darbuotojų veiksmai, susiję su kompiuterinės ir (ar) programinės įrangos naudojimu Taryboje privalo būti derinami su TVITS, administratoriais ir Tarybos informacijos saugumo įgaliotiniu.

_____

Informacijos apdorojimo priemonių naudojimo tvarkos aprašo
1 priedas

LAIKMENŲ NAIKINIMO BŪDAI

Laikmenos rūšis	**Naikinimo būdas**
Standieji diskai	1. Standieji diskai išardomi, o informacinis sluoksnis nuo pagrindo nutrinamas abrazyvinėmis priemonėmis. 2. Specialiais standžiųjų diskų mechaninio naikinimo prietaisais, kurie smulkina standžiuosius diskus ne didesnio nei 20 milimetrų pločio dalelėmis. Papildomai rekomenduojama naikinti daugiau nei vieną laikmeną, o daleles sumaišyti. 3. Specialiais išmagnetinimo prietaisais (angl. *degausser*) kartu su kitomis fizinio naikinimo arba informacinio sluoksnio gniuždymo priemonėmis
Optiniai diskai	1. Susmulkinami (supjaustomi) ne didesnėmis nei 30 kvadratinių milimetrų dalelėmis. Šis būdas negali būti taikomas *Blu-Ray* tipo optiniams diskams naikinti. 2. Sudeginami suardant medžiagos vientisumą
Magnetinės kortelės	Susmulkinamos arba pjaustomos ne didesnėmis kaip 2 milimetrų pločio juostelėmis
USB atmintinės, įvairios atminties kortelės, lustinės kortelės, pastoviosios būsenos (SSD) diskai	1. Korpusai, laikikliai išardomi, atminties lustai susmulkinami. Įsitikinama, kad susmulkinti visi atminties lustai. 2. Susmulkinami specialiais mechaninio naikinimo prietaisais, kurie smulkina atminties lustus ne didesnio nei 9 milimetrų pločio dalelėmis. 3. Kortelės gali būti susmulkinamos ne didesnėmis kaip 2 milimetrų pločio juostelėmis

_____

Informacijos apdorojimo priemonių naudojimo tvarkos aprašo
2 priedas

INFORMACIJOS, ESANČIOS DAUGKARTINIO ĮRAŠYMO LAIKMENOSE, NEATKURIAMO TRYNIMO BŪDAI

Laikmenos rūšis	**Trynimo būdas**
Standusis diskas	Informacija trinama vadovaujantis DoD 5220.22-M standarto reikalavimais.
Telekomunikacinė ir biuro įranga	Informacija ištrinama rankiniu būdu, paskui atkuriami gamykliniai parametrai
Operatyvioji atmintinė	Išjungiamas maitinimas ne trumpesniam nei 15 minučių laikui ir išimama bateriją (jeigu tokia yra)

_____

Informacijos apdorojimo priemonių naudojimo tvarkos aprašo
3 priedas

REKOMENDACIJOS PASIRENKANT TARYBOJE NAUDOJAMAS KRIPTOGRAFINES PRIEMONES

1. Renkantis Tarybos IT infrastruktūroje, kompiuteriniame tinkle, elektroninės informacijos saugumui užtikrinti naudojamą techninę ar programinę įrangą, kurioje turi būti naudojamos kriptografinės priemonės ir (ar) mechanizmai (toliau – kriptografinė įranga), rekomenduojama rinktis:

1.1. į 2018 m. lapkričio 20 d. Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos direktoriaus įsakymu Nr. 1-61 patvirtintą Leistinų naudoti Lietuvos Respublikoje kriptografinių priemonių sąrašą (toliau – Sąrašas), įtrauktą įranga, užtikrinančią elektroninės informacijos, žymimos slaptumo žyma „Riboto naudojimo“ apsaugą. Sąrašas yra pateikiamas Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos interneto svetainėje adresu:
https://www.nksc.lt/doc/Leistinų%20naudoti%20LR%20kriptografinių%20priemonių%20sąrašas.pdf;

1.2. žinomų gamintojų įrangą, pvz., būti įtraukta į oficialų Šiaurės Atlanto sutarties organizacijos Ryšių ir informacijos agentūros Kibernetinio saugumo pajėgumų plėtros grupės interneto svetainėje skelbiamą informacijos saugą užtikrinančių gaminių katalogą (angl. *NATO Information Assurance Product Catalogue*), kurio interneto svetainės adresas https://www.ia.nato.int/niapc/

2. Tarybos veikloje gali būti naudojami simetriniai ir (arba) asimetriniai šifrai:

2.1. Simetriniai šifrai – šifrai, naudojantys tą patį raktą duomenų šifravimui ir dešifravimui. Jį gauna duomenų siuntėjas ir gavėjas. Duomenims užšifruoti prieš siunčiant ir gautiems užšifruotiems duomenims iššifruoti naudojamas tas pats šifras (raktas). Simetriniai šifrai turi naudoti ne mažesnį nei 128 bitų raktą. Tarybos veikloje turi būti naudojami šie simetriniai šifrai:

2.1.1. Blokiniai:

2.1.1.1. AES (*Advanced Encryption Standard*). Rakto dydis 128 bitai ir daugiau;

2.1.1.2. *Triple-DES* (3DES arba TDEA), esant galimybei turėtų būti keičiamas į AES.

2.1.2. Srautiniai (kai srautas šifruojamas po vieną bitą vienu metu): *Rivest Cypher 4* (RC4) su 128 bitų raktu, jei nėra galimybės migruoti į AES blokinį šifrą.

2.2. Asimetriniai šifrai – šifrai, naudojantys šifravimui viešą ir privatų raktus. Šiame šifravimo metode generuojami du tarpusavyje susiję raktai. Jei duomenys užšifruojami vienu raktu, tai juos iššifruoti įmanoma tik kitos poros raktu. Žinant tik vieną poros raktą, neįmanoma atstatyti kito rakto. Tarybos veikloje asimetriniam šifravimui gali būti naudojami šie asimetriniai šifrai:

2.2.1. RSA su ne trumpesniu nei 1024 bitų raktu;

2.2.2. ECC su 224 arba 256 bitų raktu.

3. Rekomenduojama naudoti šiuos maišos (angl. *hash*) algoritmus:

3.1. SHA – 256;

3.2. SHA – 384;

3.3. SHA – 512;

3.4. Whirlpool (10 ir daugiau etapų);

3.5. RIPEMD – 160.

4. Šifravimui negali būti naudojami šių maišų algoritmai:

4.1. SHA – 1;

4.2. MD5.

Informacijos apdorojimo priemonių naudojimo
tvarkos aprašo
4 priedas

KRIPTOGRAFINIŲ PRIEMONIŲ APSKAITOS ŽURNALAS

Eil. Nr.	Data	Kriptografinės priemonės pavadinimas	Serijos Nr.	Inventorinis Nr.	Asmens, kuriam išduota kriptografinė priemonė vardas, pavardė, pareigos, parašas	Išdavimo data	Grąžinimo data	Pastabos
1	2	3	4	5	6	7	8	9

_____