PATVIRTINTA
Nacionalinio maisto ir veterinarijos
rizikos vertinimo instituto direktoriaus
2022 m. vasario 3 d. įsakymu Nr. 1A-21

NACIONALINIO MAISTO IR VETERINARIJOS RIZIKOS VERTINIMO INSTITUTO TVARKOMŲ REGISTRŲ IR INFORMACINIŲ SISTEMŲ SAUGAUS ELEKTRONINĖS INFORMACIJOS TVARKYMO TAISYKLĖS

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Nacionalinio maisto ir veterinarijos rizikos vertinimo instituto (toliau – NMVRVI) tvarkomų registrų ir informacinių sistemų saugaus elektroninės informacijos tvarkymo taisyklių (toliau — taisyklės) tikslas — sudaryti sąlygas saugiai tvarkyti Laboratorijos informacijos valdymo sistemos, Veterinarinės informacijos valdymo sistemos, Kokybės dokumentų informacinės valdymo sistemos, Norminių dokumentų valdymo informacinės sistemos, Rivilė – buhalterinės apskaitos, finansų ir verslo valdymo sistemos, Finansų valdymo ir apskaitos informacinės sistemos, Dokumentų valdymo sistemos (toliai – IS) elektroninę informaciją bei nustatyti techninius ir kitus elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus.

2. Taisyklėse vartojamos sąvokos atitinka sąvokas, apibrėžtas Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, Saugos dokumentų turinio gairių apraše, Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, ir kitų informacinių sistemų klasifikavimo gairių apraše, patvirtintuose Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimą 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“, Techniniuose va1stybės registrų (kadastrų), žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašuose, patvirtintuose Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „.Dėl Techninių valstybės registrų (kadastrų), Žinybinių registrų, valstybės informacinių sistemų ir kitų informacinių sistemų elektroninės informacijos saugos reikalavimų aprašo ir informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo" (toliau – Reikalavimai), NMVRVI tvarkomų registrų ir informacinių sistemų duomenų saugos nuostatuose (toliau — Duomenų saugos nuostatai) ir kituose teisės aktuose.

3. Informacinėse sistemose tvarkoma elektroninė informacija ir jos grupių sąrašas ir svarbos kategorijos nurodomi informacinių sistemų nuostatuose.

4. Už NMVRVI informacinėse sistemose esančios elektroninės informacijos, priskirtos svarbios elektroninės informacijos kategorijai, tvarkymą atsakingi NMVRVI direktoriaus paskirti valstybės tarnautojai ir/arba darbuotojai, dirbantys pagal darbo sutartis.

5. Informacinių sistemų naudotojai, pagal kompetenciją tvarkantys elektroninę informaciją (įskaitant ir tvarkančius informacinių sistemų duomenis pagal pasirašytas sutartis) ir atsakantys už elektroninės informacijos tvarkymą, nurodyti informacinių sistemų nuostatuose.

6. NMVRVI informacinių sistemų bei registrų administratorių, kompiuterinio tinklo bei techninės įrangos administratorių, kompiuterių saugumo incidentų tyrimo grupių narių, informacinių technologijų bei telekomunikacijų, taip pat informacinių sistemų ir/arba registrų priežiūros, palaikymo ir/arba vystymo paslaugų teikėjų ir/arba techninės įrangos tiekimo, priežiūros ir/arba palaikymo paslaugų tiekėjų (toliau kartu vadinami Tiekėjais, o kiekvienas atskirai - Tiekėju) atliekami veiksmai, kurių metu vykdomas asmens duomenų tvarkymas, galimi tik tiek, kiek tai yra būtina ir proporcinga, siekiant užtikrinti tinklo ir informacijos saugumą, t. y.

tinklo ar informacinės sistemos atsparumą (pagal nustatytą patikimumo laipsnį) trikdžiams arba neteisėtiems tyčiniams ir/arba netyčiniams veiksmams, kuriais pažeidžiamas saugomų ar persiunčiamų asmens duomenų prieinamumas, autentiškumas, vientisumas ir/arba konfidencialumas, ir susijusių paslaugų, kurias teikia tie tinklai ir sistemos arba kurios per juos prieinamos, saugumą, laikomas teisėtu atitinkamo duomenų valdytojo interesu (pvz., užkirsti kelią neteisėtai prieigai prie elektroninių ryšių tinklų ir/arba kenkimo programų kodų platinimui, taip pat sustabdyti atkirtimo nuo paslaugos atakas ir neleisti pakenkti kompiuterių bei elektroninių ryšių sistemoms ir pan.).

II SKYRIUS
TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS

7. Kompiuterinės įrangos saugos priemonės:

7.1. tarnybinių stočių svarbiausios funkcijos turi būti dubliuojamos;

7.2. naudotojų kompiuteriuose turi būti naudojama tik legali ir darbo funkcijoms atlikti reikalinga programinė įranga pagal patvirtintą leistinos programinės įrangos sąrašą;

7.3. tarnybinėse stotyse ir naudotojų kompiuteriuose turi būti įdiegtos centralizuotai valdomos ir nuolat atnaujinamos kenksmingos programinės įrangos aptikimo ir stebėjimo realiu laiku programos;

7.4. rekomenduotina, kad įsilaužimo atakų pėdsakai (angl. attack signature) būtų atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius.

7.5. informacinių sistemų komponentų stebėjimo priemonės turi perspėti informacinės sistemos administratorių, kai pagrindinėje informacinių sistemų kompiuterinėje įrangoje iki nustatytos pavojingos ribos sumažėja laisvos kompiuterio atminties ar vietos diske, ilgą laiką stipriai apkraunamas centrinis procesorius ar kompiuterio tinklo sąsaja, sutrinka kitų informacinių sistemų komponentų įprastas veikimas;

7.6. prieiga prie IS naudotojų darbo vietų yra kontroliuojama.

8. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

8.1. Informacinių sistemų tarnybinėse stotyse ir vidinių informacinių sistemų naudotojų darbo kompiuteriuose naudojamos centralizuotai valdomos ir atnaujinamos kenksmingosios programinės įrangos aptikimo, stebėjimo realiu laiku priemonės. Šios priemonės automatiškai turi informuoti informacinės sistemos administratorių apie tai, kuriems informacinių sistemų posistemiams, funkciškai savarankiškoms sudedamosioms dalims yra pradelstas kenksmingosios programinės įrangos aptikimo priemonių atsinaujinimo laikas;

8.2. programinės įrangos diegimą, šalinimą ir konfigūravimą turi teisę atlikti tik IS administratorius arba kitas įgaliotas asmuo;

8.3. programinė įranga turi turėti apsaugą nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. SQL injection), XSS (angl. Cross-site scripting), atkirtimo nuo paslaugos (angl. DOS), dedikuoto atkirtimo nuo paslaugos (angl. DDOS) ir kitų;

8.4. rekomenduotina informacinės sistemos tinklo perimetro apsaugai naudoti filtrus, apsaugančius elektroniniame pašte ir viešame ryšių tinkle naršančių informacinės sistemos naudotojų kompiuterinę įrangą nuo kenksmingo kodo;

8.5. vidinių informacinių sistemų naudotojo darbo vietose gali būti naudojamos tik tarnybos (darbo) reikmėms skirtos išorinės duomenų laikmenos (pvz., USB atmintinės, kompaktiniai diskai ir kt.). Šios laikmenos negali būti naudojamos veiklai, nesusijusiai su teisėtu informacinių sistemų tvarkymu;

8.6. programinės įrangos testavimas turi būti atliekamas tam tikslui skirtoje testavimo aplinkoje, nenaudojant realių asmens duomenų ar kitos realios konfidencialios arba atitinkamo slaptumo lygio informacijos;

9. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

9.1. elektroninės informacijos perdavimo tinklo mazgai turi turėti rezervinį maitinimo šaltinį, užtikrinantį jų veikimą ne trumpiau kaip 30 minučių;

9.2. elektroninės informacijos perdavimo tinklo mazgai ir ryšio linijos turi būti dubliuoti ir jų techninė būklė nuolat stebima;

9.3. kitoms valstybės institucijoms, valstybės registrams ir valstybės informacinėms sistemoms, kitoms informacinėms sistemoms informacinių sistemų elektroninė informacija turi būti perduodama saugiais elektroninių ryšių tinklais;

10. Patalpų ir aplinkos saugumo užtikrinimo priemonės:

10.1. turi būti įrengta patalpų apsaugos signalizacija, kurios signalai turi būti persiunčiami patalpas saugančiai saugos tarnybai;

10.2. patalpos turi būti suskaidytos į sektorius. Teisė atrakinti ir (ar) užrakinti tam tikrą sektorių turi būti suteikiama tik darbuotojams, kurie atlikdami tarnybines funkcijas būtinai turi lankytis tame sektoriuje;

10.3. patalpose turi būti įrengta įeigos kontrolės elektroninė sistema;

10.4. patalpos ir konkretūs jų sektoriai turi būti saugiai užrakinami, langai ir durys tinkamai apsaugoti nuo nesankcionuotos fizinės prieigos naudojant užraktus, apsaugos signalizaciją, vaizdo stebėjimo kameras;

10.5. paliekant patalpas ar darbo vietas turi būti užrakinamos durys ir uždaromi langai;

10.6. visi lankytojai turi būti lydimi NMVRVI darbuotojų, išskyrus atvejus, kai tokia lankytojų prieiga yra iš anksto patvirtinta;

10.7. informacinių sistemų naudotojų darbo vietų aplinka turi atitikti Lietuvos higienos normą HN 32:2004 „Darbas su video terminalais. Saugos ir sveikatos reikalavimai“, patvirtintą Lietuvos Respublikos sveikatos apsaugos ministro 2004 m. vasario 12 d. įsakymu Nr. V-65 „Dė1 Lietuvos higienos normos HN 32:2004 „Darbo su video terminalais. Saugos ir sveikatos reikalavimai“ patvirtinimo“, ir kitus Lietuvos Respublikos teisės aktuose nustatytus reikalavimus;

10.8. visose patalpose ir konkrečiuose jų sektoriuose turi būti ugnies gesintuvai, įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato apsaugos signalizacijos ir saugos tarnybos stebėjimo pulto, reguliariai atliekama gaisro aptikimo ir gesinimo priemonių patikra.

11. Papildomos tarnybinių stočių patalpų apsaugos nuo neteisėto asmenų patekimo į jas ir kitos saugos užtikrinimo priemonės:

11.1. patalpa turi būti prijungta prie atskiros signalizacijos zonos;

11.2. patalpose turi būti dubliuota oro kondicionavimo ir drėgmės kontrolės įranga. Temperatūros ir oro drėgnumo normos turi būti užtikrinamos pagal techninės įrangos gamintojo nustatytus reikalavimus. Patalpų oro kondicionavimo ir drėgmės kontrolės įranga turi turėti automatinę įspėjimo funkciją. Apie neužtikrinamas patalpą oro temperatūros ir oro drėgnumo normas turi būti automatiškai informuojami informacinių sistemų administratoriai, atliekantys techninės įrangos priežiūrą;

11.3. patalpose turi būti užtikrinamas nepertraukiamas elektros energijos tiekimas, naudojant alternatyvų elektros energijos tiekimo ša1tinį, kurio veikimas turi būti tikrinamas ne rečiau kaip kartą per mėnesį imituojant elektros energijos dingimą;

11.4. fizinė prieiga prie patalpos suteikiama tik NMVRVI direktoriaus įsakymu paskirtiems atsakingiems darbuotojams. Kiti darbuotojai arba tretieji asmenys gali patekti į šią patalpą tik lydimi atsakingų darbuotojų. Kiekvienas patekimas į patalpą turi būti fiksuojamas;

11.5. tarnybinių stočių patalpų raktai turi būti saugomi. Rekomenduojama, kad pagrindiniai tarnybinių stočių patalpos raktai ir atsarginiai raktai būtų saugomi atskiruose pastatuose;

11.6. patalpoje neturi būti langų arba naudojami didelio atsparumo langai specialiais rėmais ir grotomis;

11.7. patalpos durys privalo būti šarvuotos ir apsaugotos bent dviem skirtingos konstrukcijos spynomis, jos visada rakinamos;

11.8. kompiuterinio ryšio linijos apsaugotos nuo elektros išlydžių, perkūnijos ir elektros linijų avarijų naudojant apsauginius įtaisus su įžeminimo tašku.

12. Informacinių sistemų veikimo užtikrinimas:

12.1. pirmosios kategorijos informacinės sistemos vienkartinis neveikimo laikotarpis negali būti ilgesnis nei 8 val.;

12.2. antrosios kategorijos informacinių sistemų vienkartinis neveikimo laikotarpis negali būti ilgesnis nei 12 val.;

12.3. trečios kategorijos informacinių sistemų neveikimo laikotarpis negali būti ilgesnis

nei 16 val.;

12.4. ketvirtos kategorijos informacinių sistemų neveikimo laikotarpis negali būti ilgesnis nei 24 val.

12.5. per metus turi būti užtikrintas informacinės sistemos prieinamumas: ketvirtos kategorijos informacinėms sistemoms – ne mažiau kaip 70 proc. laiko darbo metu darbo dienomis, trečios kategorijos informacinėms sistemoms – ne mažiau kaip 90 proc. laiko darbo metu darbo dienomis, antros kategorijos informacinėms sistemoms – ne mažiau kaip 96 proc. laiko visą parą, pirmos kategorijos informacinėms sistemoms – ne mažiau kaip 99 proc. laiko visą parą.

III SKYRIUS
SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS

16. Saugaus elektronines informacijos keitimo, atnaujinimo, įvedimo ir naikinimo tvarka:

16.1. informacinės sistemos elektroninę informaciją įvesti, keisti, atnaujinti ir naikinti gali tik autorizuoti informacinės sistemos naudotojai, turintys teisę atlikti šiuos veiksmus ir pasirašę pasižadėjimą laikytis informacinės sistemos saugos reikalavimų.

16.2. elektroninė informacija į informacinės sistemas gali būti įvedama, jose keičiama, atnaujinama ir naikinama tik šių taisyklių, atitinkamų NMVRVI valdomų informacinių sistemų nuostatų, ir kitų teises aktų, reglamentuojančių informacinių sistemų veiklą ir elektroninės informacijos tvarkymą, nustatyta tvarka;

16.3. elektroninė informacija gali būti tvarkoma, tik vykdant pareigybės aprašyme nustatytas funkcijas arba gavus teisėtą įgalioto asmens pavedimą ir tik turint teisėtą tikslą ir pagrindą, taip pat tik ta apimtimi, kuri reikalinga tarnybinėms funkcijoms atlikti;

16.4. informacinėse sistemose esančiomis elektroninės informacijos naikinimo priemonėmis turi būti užtikrinta, kad nebūtų galima atkurti galutinai sunaikintos elektroninės informacijos;

16.5. informacinių sistemų naudotojui neatliekant jokių veiksmų informacinėse sistemose 15 minučių, informacinių sistemų taikomoji programinė įranga turi užsirakinti, kad toliau naudotis informacinėmis sistemomis galima būtų tik pakartotinai atlikus savo tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

16.6. baigus darbą ar pasitraukus iš darbo vietos informacinėse sistemose turi būti imamasi priemonių, kad su elektronine informacija negalėtų susipažinti pašaliniai asmenys: atsijungiama nuo informacinių sistemų, įjungiama ekrano užsklanda su slaptažodžiu, dokumentai ar jų kopijos darbo vietoje turi būti padedami į pašaliniams asmenims neprieinamą vietą;

16.7. informacinės sistemos turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo, patikimumo tikrinimo ir informavimo apie klaidas priemones;

17. Atsarginių elektroninės informacijos kopijų darymas, saugojimas, elektroninės informacijos atkūrimo iš atsarginių kopijų išbandymas vykdomas, vadovaujantis sutarčių su išoriniais paslaugų teikėjais nuostatomis.

18. Elektroninė informacija perkeliama ir teikiama susijusiems registrams ar kitoms informacinėms sistemoms ir iš jų gaunama vadovaujantis nurodytuose teisės aktuose nustatyta tvarka ir sąlygomis.

19. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo, perdavimo ar kitokios neteisėtos veiklos (toliau — neteisėta veikla) nustatymo tvarka ir priemonės:

19.1. informacinių sistemų naudotojai, pastebėję saugos dokumentuose arba kibernetinio saugumo dokumentuose nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos (kibernetinio saugumo) užtikrinimo priemones, įvykius ar veiką, atitinkančią kibernetinio ar elektroninės informacijos saugos incidento požymius, arba apie tai gavę informacijos iš kitų informacijos šaltinių, privalo nedelsdami apie tai pranešti informacinių sistemų administratoriams arba tiesiogiai informuoti saugos įgaliotinius;

19.2. saugos įgaliotinis, įtaręs, kad su elektronine informacija vykdoma neteisėta veikla, inicijuoja elektroninės informacijos saugos incidentų valdymo procedūras;

19.3. informacinių sistemų programinės ir techninės įrangos keitimo, informacinių sistemų pokyčių valdymo tvarka nustatyta sutartyse su išoriniais paslaugų teikėjais ir/arba reglamentuose, suderintuose su išoriniais paslaugų teikėjais.

20. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių (toliau — mobilieji įrenginiai) naudojimo tvarka:

20.1. mobiliesiems įrenginiams, naudojamiems NMVRVI patalpose, esantiems vidiniame informacinių sistemų kompiuterio tinkle, taikomi tokie patys elektroninės informacijos saugos (kibernetinio saugumo) reikalavimai, kaip ir stacionariesiems kompiuteriams;

20.2. iš mobiliųjų įrenginių draudžiama tiesiogiai nuotoliniu būdu prisijungti prie informacinių sistemų informacinių technologijų infrastruktūros. Prisijungimas galimas tik virtualiojo privačiojo tinklo ryšiu per tarpinį įrenginį, atitinkantį saugos politiką įgyvendinančiuose dokumentuose nustatytus organizacinius ir techninius elektroninės informacijos saugos (kibernetinio saugumo) reikalavimus;

20.3. rekomenduojama reguliariai tikrinti tarpinius įrenginius, saugos įgaliotiniui arba informacinės sistemos administratoriui pranešti apie neleistinus ar saugumo reikalavimų neatitinkančius tarpinius įrenginius;

20.4. mobilieji įrenginiai, kuriais naršoma internete, privalo būti apsaugoti nuo judriųjų programų (angl. mobile code) keliamos grėsmės;

20.5. mobiliuosiuose įrenginiuose turi būti naudojamos vykdomojo kodo (angl. executable code) kontrolės priemones, automatiškai apribojančios neleistino vykdomojo kodo naudojimą ar informacinės sistemos administratorių informuojančios apie neleistino vykdomojo kodo naudojimą;

20.6. mobiliuosiuose įrenginiuose nenaudojamos bevielio ryšio funkcijos turi būti išjungtos;

20.7. informacinių sistemų elektroninė informacija ir kita nevieša informacija, laikoma mobiliuosiuose įrenginiuose, turi būti užšifruota. Mobiliuose įrenginiuose, jeigu jie naudojami ne NMVRVI patalpose, draudžiama saugoti ypatingus asmens duomenis;

20.8. mobiliųjų įrenginių kenksmingosios programinės įrangos aptikimo, elektroninės informacijos šifravimo ir kita programinė įranga turi būti įsigyjama tik iš patikimų ir oficialių Tiekėjų teisės aktų nustatyta tvarka;

20.9. mobilieji įrenginiai viešose vietose negali būti palikti be priežiūros. Mobilusis įrenginys, kuriuo nesinaudojama 15 min., turi automatiškai užsirakinti.

21. Tais atvejais, jei dėl asmens duomenų saugumo pažeidimo būtų prarasti asmens duomenys, NMVRVI nedelsdama turi pranešti duomenų subjektui apie asmens duomenų saugumo pažeidimą, kai dėl to asmens duomenų saugumo pažeidimo gali kilti didelis pavojus fizinio asmens teisėms ir laisvėms, kad jis galėtų imtis reikiamų priemonių užkirsti tam kelią. Pranešime turėtų būti aprašytas asmens duomenų saugumo pažeidimo pobūdis ir pateiktos atitinkamam fiziniam asmeniui skirtos rekomendacijos, kaip sumažinti galimą neigiamą poveikį. Taip pat ne vėliau kaip per 72 val. informuojama Valstybinė duomenų apsaugos inspekcija jos nustatyta tvarka ir forma.

22. Darbuotojų nuotolinio darbo tvarka:

22.1. darbuotojai, savo darbui skirtą kompiuterinę įrangą gali išsinešti tik darbuotojui pasirašius priėmimo – perdavimo aktą, kuriuo darbuotojas prisiima atsakomybę už nešiojamą kompiuterį ir kitą, įstaigai priklausantį turtą.

22.2. darbuotojams skirti kompiuteriai turi būti parengti ir sukonfigūruoti veikti slaptažodžiais apsaugotomis paskyromis.

22.3. darbuotojai dirbantys nuotoliniu būdu, turi naudoti virtualų saugųjį tinklą (angl. Virtual private network) arba kitą IS administratoriaus suteiktą, saugų duomenų perdavimą užtikrinantį būdą.

22.4. kompiuterinė įranga, kai su ja nedirbama, turi būti laikoma saugioje vietoje, kur ja negalėtų pasinaudoti asmenys, kuriems ji nėra suteikta.

IV SKYRIUS
REIKALAVIMAI, KELIAMI INFORMACINĖMS SISTEMOMS FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR TEIKĖJAMS

23. Reikalavimai informacinėms sistemoms funkcionuoti ir reikalingoms paslaugoms (projektvaimo, aptarvavimo ir priežiūros) veikti, nustatomi tiekėjams paslaugų teikimo sutartyse.

24. NMVRVI privalo užtikrinti, kad:

24.1. Tiekėjai atitiktų informacinių sistemų veiklą reglamentuojančių teisės aktų, standartų, šių taisyklių reikalavimus ir paslaugų teikimo, darbų atlikimo ar įrangos tiekimo pirkimo dokumentuose iš anksto nustatomus reikalavimus Tiekėjo kompetencijai, patirčiai, teikiamoms paslaugoms, atliekamiems darbams ar tiekiamai įrangai;

24.2. perkamos paslaugos, darbai ar įranga, susiję su informacinėmis sistemomis, atitiktų teisės aktų ir standartų, kuriais vadovaujamasi užtikrinant informacinių sistemų elektroninės informacijos saugą (kibernetinį saugumą), reikalavimus, kurie iš anksto nustatomi paslaugų teikimo, darbų atlikimo ar įrangos tiekimo pirkimo dokumentuose;

24.3. Tiekėjas, vykdydamas sutartinius įsipareigojimus, įgyvendintų tinkamas organizacines ir technines priemones, skirtas informacinėms sistemoms ir jose tvarkomai elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

25. Tiekėjai į tarnybinių stočių patalpas įleidžiami, tik lydint įgaliotam sistemų administratoriui ar kitam įgaliotam NMVRVI valstybės tarnautojui.

26. Tiekėjui prieiga prie informacinių sistemų gali būti suteikiama, tik pasirašius sutartį, kurioje turi būti nustatytos Tiekėjo teisės, pareigos, prieigos prie informacinių sistemų lygiai ir sąlygos, elektroninės informacijos saugos (kibernetinio saugumo), konfidencialumo reikalavimai ir atsakomybė už jų nesilaikymą. Informacinės sistemos administratorius turi supažindinti Tiekėją su suteiktos prieigos prie informacinių sistemų saugos (kibernetinio saugumo) reikalavimais ir sąlygomis, taip pat Tiekėjo įgaliotas asmuo turi būti supažindinamas pasirašytinai su duomenų saugos reikalavimais ir atsakomybe už šių reikalavimų pažeidimus.

27. Informacinės sistemos administratorius suteikia prieigos prie informacinės sistemos duomenų teisę (peržiūrėti duomenis, atlikti užklausas, vykdyti veiksmus su sistemos duomenimis ir kt.) ir fizinę prieigą prie techninės ir programinės įrangos paslaugų teikėjo įgaliotam fiziniam asmeniui paslaugų teikimo sutartyje nurodytam laikotarpiui jam nustatytoms funkcijoms atlikti.

28. Iškilus poreikiui, siekdama įsitikinti, ar tinkamai vykdoma sutartis, ar laikomasi elektroninės informacijos saugos (kibernetinio saugumo) reikalavimų, NMVRVI turi teisę atlikti Tiekėjo teikiamą paslaugų stebėseną ir auditą, suteikti galimybę atlikti auditą trečiosioms šalims.

29. Pasibaigus paslaugų teikimo sutartyje nurodytam laikotarpiui. IS administratorius panaikina paslaugų tiekėjo įgaliotų asmenų prieigos prie IS programinių, techninių ir kitų resursų teises ir apie tai juos informuoja.

_____