PATVIRTINTA

 Viešosios įstaigos Vilniaus miesto

 klinikinės ligoninės direktoriaus

 2022 m. balandžio 15 d. įsakymu Nr.V1-114/22(1.1.)

**VMKL INFORMACINĖS SISTEMOS**

**Saugaus elektroninės informacijos tvarkymo taisyklės**

**I SKYRIUS**

**BENDROSIOS NUOSTATOS**

1. Viešosios įstaigos Vilniaus miesto klinikinė ligoninė (toliau – VMKL) valdomos ir tvarkomos informacinės sistemos (toliau – IS) saugaus elektroninės informacijos tvarkymo taisyklių (toliau – Taisyklės) tikslas – nustatyti elektroninės informacijos tvarkymo, techninius ir kitus elektroninės informacijos saugos ir kibernetinio saugumo reikalavimus.

2. Taisyklėse vartojamos sąvokos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Bendrųjų elektroninės informacijos saugos reikalavimų apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2013 m. liepos 24 d. nutarimu Nr. 716 „Dėl Bendrųjų elektroninės informacijos saugos reikalavimų aprašo, Saugos dokumentų turinio gairių aprašo ir Elektroninės informacijos, sudarančios valstybės informacinius išteklius, svarbos įvertinimo ir valstybės informacinių sistemų, registrų ir kitų informacinių sistemų klasifikavimo gairių aprašo patvirtinimo“ ir Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, patvirtintame Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“ (toliau – Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, aprašas).

3. IS tvarkoma elektroninė informacija ir jos grupių sąrašas:

3.1. Viešosios įstaigos Vilniaus miesto klinikinės ligoninės informacinėje sistemoje tvarkomi su asmens sveikatos priežiūros paslaugų teikimu susiję duomenys;

3.2. VMKL internetinės svetainės informacinėje sistemoje tvarkoma viešosios komunikacijos informacija bei informacija pagal Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms ir mobiliosioms programoms aprašo, patvirtinto Lietuvos Respublikos Vyriausybės 2003 m. balandžio 18 d. Nr. 480 „Dėl Bendrųjų reikalavimų valstybės ir savivaldybių institucijų ir įstaigų interneto svetainėms aprašo patvirtinimo“;

3.3. El. pašto sistemoje tvarkoma elektroninės komunikacijos informacija;

3.4. Buhalterinės apskaitos IS „Rivile“ tvarkomi finansinės ir buhalterinės apskaitos duomenys;

3.5. Dokumentų valdymo IS „DVS“ tvarkomi gaunamų ir siunčiamų dokumentų bei VMKL teisės aktų duomenys;

3.6. Personalo valdymo IS „PVS“ tvarkomi darbuotojų duomenys;

4. Už IS esančios elektroninės informacijos, priskirtos vidutinės svarbos elektroninės informacijos kategorijai, tvarkymą yra atsakingi IS naudotojai ir IS administratoriai.

**II SKYRIUS**

**TECHNINIŲ IR KITŲ SAUGOS PRIEMONIŲ APRAŠYMAS**

5. Tarnybinių stočių, kompiuterinių darbo vietų, mobilių įrenginių, terminalų, informacinių ekranų (toliau - kompiuterinės įrangos) saugos priemonės:

5.1. kompiuterinė įranga eksploatuojama ir prižiūrima laikantis gamintojo reikalavimų;

5.2. kompiuterinės įrangos gedimai ir keitimai yra registruojami;

5.3. tarnybinių stočių pagrindinė techninė įranga privalo turėti įtampos filtrą ir rezervinį maitinimo šaltinį, užtikrinantį VMKL IS veikimą ne mažiau kaip 30 min.;

5.4. darbo reikmėms naudojamų mobilių įrenginių atminties laikmenos užšifruojamos;

5.5. darbo vietų kompiuterinėje įrangoje įjungta lokali ugniasienė ir sukonfigūruota taip, kad ribotų visą VMKL IS veikimui nereikalingą srautą, nenaudojamus prievadus, protokolus ir paslaugas;

5.6. tarnybinėse stotyse įjungta išorinė ugniasienė, ribojanti prieigą prie viešojo kompiuterių tinklo;

5.7. ryšiui tarp duomenų bazių tarnybinių stočių ir taikomųjų programų serverių naudojami nestandartiniai TCP/UDP prievadai arba kitos ryšio priemones;

5.8. administruojant kompiuterinę įrangą naudojami saugūs, šifruoti kanalai;

5.9. IS naudotojai ir IS administratoriai užtikrina naudojamos kompiuterinės įrangos, mobilių įrenginių fizinę apsaugą:

5.9.1. negalima palikti be priežiūros neapsaugotą darbo vietos kompiuterinę įrangą, mobilius įrenginius;

5.9.2. išeinant iš patalpų, kurioje yra kompiuterinė įranga, nepaliekami pašaliniai asmenys, įsitikinama, kad langai uždaryti ir durys užrakintos.

5.10. turi būti įdiegtos ir veikti automatizuotos įsibrovimo aptikimo sistemos, kurios stebėtų IS gaunamą ir išsiunčiamą duomenų srautą bei vidinį srautą tarp svarbiausių tinklo paslaugų;

6. Sisteminės ir taikomosios programinės įrangos saugos priemonės:

6.1. programinė įranga turi būti prižiūrima ir savalaikiai atnaujinama laikantis gamintojo reikalavimų ir rekomendacijų;

6.2. operacinės sistemos konfigūruojamos laikantis gamintojo saugios konfigūracijos rekomendacijų;

6.3. kompiuterinėje įrangoje naudojama tik tokios operacinių sistemų versijos, kurias palaiko gamintojai, t.y. periodiškai išleidžia programinės įrangos pataisymus. Operacinių sistemų pataisymai diegiami užtikrinant jų savalaikiškumą;

6.4. naudojama tik legali, patikimų gamintojų ir tik tiesiogiai darbo funkcijos atlikti ar VMKL IS funkcionalumui užtikrinti reikalinga programinė įranga;

6.5. IS administratorius reguliariai, ne rečiau kaip kartą per mėnesį, įvertina informaciją apie neįdiegtus rekomenduojamus gamintojų atnaujinimus ir susijusius saugos pažeidžiamumų svarbos lygius. Vadovaujantis saugos pažeidžiamumų svarbos lygiais IS administratorius ištestuoja ir įdiegia naudojamos programinės įrangos gamintojų atnaujinimus;

6.6. programinės įrangos atnaujinimai, nauja diegiama programinė įranga ir konfigūraciniai pakeitimai testuojami naudojant atskirą testavimui skirtą aplinką;

6.7. programinės įrangos diegimą, konfigūravimą ir šalinimą atlieka tik IS administratorius ar kiti įgalioti asmenys. IS naudotojams draudžiama kopijuoti, trinti ar savavališkai įdiegti bet kokią programinę įrangą, įskaitant ir platinimą internetu;

6.8. VMKL IS sisteminės ir taikomosios programinės įrangos keitimai yra registruojami;

6.9. kiekvienas IS naudotojas ir IS administratorius sistemoje unikaliai identifikuojamas - savo tapatybę patvirtinta naudotojo vardu ir slaptažodžiu;

6.10. tarnybinėse stotyse įjungta audito funkcija, fiksuojanti sisteminiuose žurnaluose visus tarnybinių stočių ir IS naudotojų bei IS administratorių veiksmus;

6.11. IS naudotojo ir IS administratoriaus teisė naudotis sistema panaikinama pasibaigus darbo santykiams ar gavus tiesioginio vadovo nurodymą panaikinti teisę naudotis sistema;

6.12. IS programinė įranga naudojama griežtai tik darbo funkcijoms atlikti;

6.13. IS naudotojui baigus darbą su VMKL IS imamasi šių priemonių, kad su VMKL IS saugoma elektronine informacija negalėtų susipažinti pašaliniai asmenys:

6.13.1. VMKL IS darbo vietos kompiuteryje įjungiama ekrano užsklanda su slaptažodžiu;

6.13.2. automatiškai nutraukiama sesija, naudotojui tam tikrą laiką nesinaudojant VMKL IS, kad norint pratęsti darbą iš naujo reiktų patvirtinti IS naudotojo tapatybę;

6.14. tarnybinėse stotyse, kompiuterinėse darbo vietose įjungta automatinio užrakinimo funkcija, kuri įsijungia, jeigu 15 minučių neatliekami jokie veiksmai;

6.15. VMKL IS saugomi asmens duomenys bei duomenys, kuriuose yra jauti informacija, šifruojami;

6.16. Kompiuterinėje įrangoje (kai yra techninės galimybės) naudojamos centralizuotai valdomos kenksmingos programinės įrangos aptikimo priemonės, kurios:

6.16.1. nuolat ieško ir blokuoja kenksmingą programinę įrangą (virusų, šnipinėjimo programinę įrangą ir kt.);

6.16.2. kenksmingos programinės įrangos parašai ir paieškos variklis reguliariai atnaujinamas kas 8 val. automatiniu būdu arba inicijavus IS administratoriui, iš centrinės valdymo sistemos;

6.16.3. aptikus kenksmingą programinę įrangą automatiškai pranešama IS administratoriui apie saugos incidentą bei atliekami įrašai įvykių žurnale;

6.17. IS naudotojai neturi prieigos teisės keisti nustatymus arba išjungti kenksmingos programinės įrangos aptikimo priemones;

6.18. kompiuterinė įranga neeksploatuojamos be kenksmingos programinės įrangos aptikimo priemonių, nebent rizikos vertinimo metu nustatyta, kad esama rizika priimtina;

7. Elektroninės informacijos perdavimo tinklais saugumo užtikrinimo priemonės:

7.1. kompiuterių tinklas turi būti atskirtas nuo viešųjų elektroninių ryšių tinklų (interneto) naudojant ugniasienes, automatinę įsilaužimų aptikimo ir prevencijos įrangą, atkirtimo nuo paslaugos, dedikuoto atkirtimo nuo paslaugos įrangą;

7.2. VMKL IS elektroninės informacijos perdavimo tinklo įrangoje, jei yra techninės galimybės, turi būti įjungta audito funkcija, fiksuojanti srauto duomenis, naudotojų, Informacinių sistemų elektroninės informacijos perdavimo tinklo įrangos veiksmus;

7.3. ugniasienės įvykių žurnalai (angl. Logs) turi būti reguliariai analizuojami, o ugniasienės saugumo taisyklės periodiškai peržiūrimos ir atnaujinamos;

7.4. konfigūruojant IS elektroninės informacijos perdavimo tinklo ugniasienes laikomasi principo „draudžiama pagal nutylėjimą“ – t. y. leidžiamas tik būtinas IS veiklai tinklo srautas;

7.5. ugniasienės konfigūravimo taisyklėse nustatyti komunikacijos ir prievadų apribojimai tarp skirtingų vidinio tinklo potinklių;

7.6. ugniasienių konfigūracija tikrinama ne rečiau kaip vieną kartą per metus;

7.7. turi būti įdiegta automatizuoto įsibrovimo užkardymo sistema (angl. Intrusion Prevention System) , kuri stebėtų įeinantį ir išeinantį Informacinių sistemų duomenų srautą ir vidinį srautą tarp svarbiausių tinklo paslaugų;

7.8. įsibrovimo užkardymo sistema turi sukurti pranešimą IS administratoriui apie įvykusią įtartiną veiklą. Pranešimas turi būti klasifikuojamas pagal užfiksuotą įvykį. Visa informacija apie įvykį turi būti užfiksuojama audito įrašuose;

7.9. įsibrovimo užkardymo sistemos įsilaužimo atakų pėdsakai (angl. attack signature) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per dvidešimt keturias valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos;

7.10. automatizuoto įsibrovimo užkardymo sistema apsaugo 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; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. The Open Web Application Security Project (OWASP) interneto svetainėje [www.owasp.org](http://www.owasp.org);

7.11. įsibrovimo užkardymo sistemos įsilaužimo aptikimo konfigūracijos ir kibernetinių incidentų aptikimo taisyklės turi būti saugomos elektronine forma atskirai nuo Įsibrovimo užkardymo sistemos;

7.12. VMKL IS elektroninės informacijos perdavimo tinklas yra segmentuotas pagal VMKL IS sudedamųjų dalių atliekamas funkcijas ir turi priskirtus IP adresų intervalus:

7.12.1. paslaugų tarnybinių stočių tinklas, skirtas taikomųjų programų tarnybinėms stotims;

7.12.2. VMKL IS kompiuterizuotų darbo vietų tinklai, skirti VMKL IS naudotojų kompiuterinėms darbo vietoms ir kompiuterinei įrangai;

7.13. nutolę VMKL IS naudotojai perduoda elektroninę informaciją naudodami saugias ryšio linijas;

7.14. nutolę VMKL IS naudotojai duomenis perduodantys ir gaunantys viešaisiais telekomunikacijų tinklais, perduodamų duomenų konfidencialumą užtikrina naudodami duomenų šifravimą;

7.15. VMKL IS taikomas elektroninės informacijos perdavimo tinklo trijų lygių saugumas – išorė/taikomosios programos/duomenų bazės - kiekvieną iš lygių atskiriant ugniasienėmis;

7.16. keitimasis informacija su kitais registrais ir informacinėmis sistemomis galimas tik naudojant saugius šifruotus ryšio kanalus (VPN, SSL) ir tarpines tarnybines stotis;

7.17. Elektroninės informacijos perdavimo tinklai stebimi šia tvarka:

7.17.1. visi tinklo įrenginiai, turintys paprastojo tinklo stebėjimo protokolo (angl. Simple Network Management Protocol (SNMP)) (arba analogišką) parinktį, stebimi tinklo priežiūros sistemos ir kilus nesklandumams automatiškai praneša apie problemą atsakingiems IS administratoriams;

7.17.2. visi ryšių kanalai stebimi tinklo priežiūros sistemos ir esant sutrikimams arba didelei apkrovai automatiškai praneša apie problemą atsakingiems IS administratoriams;

7.18. paslaugos įdiegtos Informacinių sistemų elektroninės informacijos perdavimo tinklo saugos srityse, kiekviena paslaugų grupė (aktyviųjų katalogų paslaugos, viešasis DNS, duomenų bazių serveriai, taikomųjų programų serveriai ir t.t.) turi atskirą saugos sritį;

7.19. nenaudojami Informacinių sistemų elektroninės informacijos perdavimo tinklo lizdai ir optiniai kompiuterių tinklo įrenginiai išjungti;

7.20. trečiųjų šalių nuotolinė prieiga prie IS elektroninės informacijos perdavimo tinklo užtikrinama pasitelkiant VPN technologiją ar kitus saugius komunikacijos būdus;

7.21. draudžiama suteikti galimybę prisijungti nuotoliniu būdu prie gamybos aplinkos serverių naudojant SSH, RDP ir kitus nuotolinio valdymo protokolus;

7.22. duomenų bazių serverius, kuriuose saugoma jautri informacija, draudžiama jungti prie DMZ Informacinių sistemų elektroninės informacijos perdavimo potinklio kartu su kitais Informacinių sistemų interneto ištekliais. Duomenų bazių serveriai, kuriuose saugoma jautri informacija, privalo būti jungiami į specialiai tam sukurtą atskirą virtualų kompiuterių tinklą, kuris yra apsaugotas ugniasiene;

7.23. IS naudotojų prieiga prie viešų interneto išteklių turi būti kontroliuojama per įgaliotąjį (proxy) serverį arba filtravimo mechanizmus palaikančią ugniasienę ar bet kokį kitą tam skirtą sprendimą.

7.24. IS elektroninės informacijos perdavimo tinklo perimetro apsaugai turi būti naudojami filtrai, apsaugantys elektroniniame pašte ir viešame ryšių tinkle naršančių Naudotojų kompiuterinės darbo vietos techninę įrangą nuo kenksmingo kodo.

8. VMKL IS naudojamų svetainių, pasiekiamų iš viešųjų elektroninių ryšių tinklų, saugumo ir kontrolės priemonės:

8.1. turi būti įgyvendinti atpažinties, tapatumo patvirtinimo ir naudojimosi IS saugumo ir kontrolės reikalavimai, nustatyti IS naudotojų administravimo taisyklėse;

8.2. draudžiant slaptažodžius saugoti programiniame kode;

8.3. turi būti naudojamas TLS (angl. Transport Layer Security) standartas. Naudojamas TLS 1.2 ir aukštesnis kriptografinis protokolas, draudžiama naudoti TLS1.0, TLS 1.1 ir SSL3;

8.4. visi kriptografiniai moduliai turi gebėti saugiai sutrikti (angl. fail securely);

8.5. tarnybinės stoties, kurioje yra svetainė, svetainės saugos parametrai turi būti teigiamai įvertinti naudojant NKSC rekomenduojamą testavimo priemonę;

8.6. turi būti naudojama svetainės saugasienė (angl. Web Application Firewall). Įsilaužimo atakų pėdsakai (angl. attack signature) turi būti atnaujinami naudojant patikimus aktualią informaciją teikiančius šaltinius. Naujausi įsilaužimo atakų pėdsakai turi būti įdiegiami ne vėliau kaip per 24 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos arba ne vėliau kaip per 72 valandas nuo gamintojo paskelbimo apie naujausius įsilaužimo atakų pėdsakus datos, jeigu VMKL IS valdytojo sprendimu atliekamas įsilaužimo atakų pėdsakų įdiegimo ir galimo jų poveikio VMKL IS veiklai vertinimas (testavimas);

8.7. turi būti naudojamos apsaugos nuo pagrindinių per tinklą vykdomų atakų: SQL įskverbties (angl. SQL injection), įterptinių instrukcijų atakų (angl. Cross-site scripting), atkirtimo nuo paslaugos (angl. DOS), paskirstyto atsisakymo aptarnauti (angl. DDOS) ir kitų, priemonės; pagrindinių per tinklą vykdomų atakų sąrašas skelbiamas Atviro tinklo programų saugumo projekto (angl. The Open Web Application Security Project (OWASP)) interneto svetainėje www.owasp.org.;

8.8. svetainės saugumo priemonės turi gebėti automatiškai uždrausti prieigą prie tarnybinės stoties iš IP adresų, vykdžiusių grėsmingą veiklą (nesankcionuoti mėginimai prisijungti, įterpti SQL intarpus ir panašiai);

8.9. svetainės, patvirtinančios nuotolinio prisijungimo tapatumą, draudžia automatiškai išsaugoti slaptažodžius;

8.10. svetainės administravimo darbai atliekami ne trumpesniu kaip 128 bitų raktu;

8.11. šifruojant naudojami skaitmeniniai sertifikatai išduoti patikimų sertifikavimo tarnybų. Draudžiama naudoti *self-signed* sertifikatus, išskyrus vidines informacines sistemas. Naudojamas sertifikato raktas ne trumpesnis kaip 2048 bitų. Sertifikato šifravimo maišos (angl. Hash) funkcijai naudojama SHA2 ir aukštesnis, SHA1 draudžiama naudoti;

8.12. svetainės kriptografinės funkcijos įdiegiamos tarnybinės stoties, kurioje yra svetainė, dalyje arba kriptografiniame saugumo modulyje (angl. Hardware security module);

8.13. prieiga prie privačių šifravimo raktų turi būti ribojama ir griežtai kontroliuojama. Privatūs šifravimo raktai turi būti saugomi kaip įmanoma mažesniame vietų skaičiuje – tarnybinėje stotyje ir atsarginių kopijų tarnybinėje stotyje;

8.14. draudžiama tarnybinėje stotyje saugoti sesijos duomenis (identifikatorių), pasibaigus susijungimo sesijai;

8.15. naudojama svetainės naudotojo įvedamų duomenų tikslumo kontrolė (angl. Validation);

8.16. tarnybinė stotis, kurioje yra svetainė, neturi rodyti svetainės naudotojui klaidų pranešimų apie svetainės programinį kodą ar tarnybinę stotį;

8.17. tarnybinė stotis, kurioje yra svetainė, leidžia tik svetainės funkcionalumui užtikrinti reikalingus HTTP metodus;

8.18. draudžiama naršyti svetainės aplankuose (angl. Directory browsing);

8.19. turi būti įdiegta svetainės turinio nesankcionuoto pakeitimo (angl. Defacement) stebėsenos sistema;

8.20. ne rečiau kaip kartą per mėnesį turi būti atliekama saugasienių užfiksuotų įvykių analizė ir pastebėtos neatitiktys saugumo reikalavimams šalinamos.

9. Pagrindinio IS tvarkytojo patalpų ir aplinkos saugumo užtikrinimo priemonės:

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

9.2. tarnybinių stočių ir tinklo perdavimo įranga saugoma atskiroje patalpoje ir / arba rakinamoje spintoje. Patalpos ar spintos raktai saugomi saugioje vietoje;

9.3. fizinė prieiga suteikiama tik įgaliotiems asmenims, kuriems tai būtina atliekant darbo funkcijas. Prieigos teises į VMKL IS tarnybinių stočių patalpą turi:

9.3.1. IS administratoriai;

9.3.2. saugos įgaliotinis;

9.4. trečiųjų šalių atstovai (IS techninės bei programinės įrangos, patalpų priežiūros specialistai ir kt.) į VMKL IS tarnybinių stočių ir tinklo perdavimo įrangos patalpas gali patekti ir dirbti joje tik lydimi turinčio įėjimo teisę į šias patalpas darbuotojo;

9.5. turi būti rakinamos durys, turi būti durų atidarymo signalizacija;

9.6. patalpos atitinka priešgaisrinės saugos reikalavimus, yra gaisro gesinimo priemonės, atliekama gaisro gesinimo priemonių patikra, įrengti priešgaisriniai davikliai;

9.7. gaisro ir įsilaužimo daviklių patikra vykdoma kartą per metus;

9.8. jei VMKL IS tarnybinių stočių patalpose esančios įrangos bendras galingumas būtų daugiau nei 10 kilovatų, turi būti įrengta oro kondicionavimo įranga;

9.9. gaisro ir apsauginės signalizacijos jutikliai prijungti prie pastato signalizacijos ir/arba apaugos tarnybos stebėjimo pulto;

9.10. tarnybinių stočių patalpa turi alternatyvų elektros energijos tiekimo šaltinį;

9.11. dirbant tarnybinių stočių patalpoje draudžiama:

9.11.1. atsinešti bet kokių daiktų, kurie nėra būtini darbui atlikti IS įrangai galinčių pakenkti daiktų, pvz.: degių medžiagų, gaisro pavojų didinančių pakavimo medžiagų);

9.11.2. palikti serverinėje daiktus, kurie nėra būtini įrangos priežiūrai ir kurie gali kelti pavojų techniniams ištekliams (pvz.: statyti oro aušinimo įrangą užstojančius daiktus arba palikti medžiagas, kurios didina gaisro pavojų);

9.11.3. IS įrangą statyti netinkamoje vietoje (pvz.: už maršrutizatorių arba serverių rėmų);

9.12. būnant tarnybinių stočių patalpoje būtina:

9.12.1. imtis privalomų saugumo priemonių, kurios liečiantis su IS įranga apsaugotų nuo elektrostatinės iškrovos arba neleistų jai susidaryti;

9.12.2. laikytis priešgaisrinės saugos reikalavimų;

9.12.3. laikytis Elektros įrangos saugos reikalavimų.

10. Kitų (galimų) IS tvarkytojų patalpų ir aplinkos saugumo užtikrinimo priemonės:

10.1. visose patalpose, kuriose yra IS naudotojų ir IS techninė įranga, turi būti įrengti gaisro ir įsilaužimo davikliai, prijungti prie pastato signalizacijos ir apsaugos tarnybų;

10.2. elektroninės informacijos perdavimo ryšių kabeliai turi būti apsaugoti nuo neteisėto prisijungimo ir pažeidimo.

11. Kitos priemonės, naudojamos IS elektroninės informacijos saugai ir kibernetiniam saugumui užtikrinti:

11.1. audito įrašų administravimas ir saugojimas:

11.1.1. kiekviename audito duomenų įraše turi būti fiksuojama:

11.1.1.1. įvykio data ir tikslus laikas;

11.1.1.2. įvykio rūšis / pobūdis;

11.1.1.3. IS naudotojo, IS administratoriaus ir (arba) IS įrenginio, susijusio su įvykiu, duomenys;

11.1.1.4. įvykio rezultatas;

11.1.2. registruojami veiksmai:

11.1.2.1. IS tarnybinių stočių, taikomosios programinės įrangos įjungimas, išjungimas, perkrovimas;

11.1.2.2. IS naudotojų, IS administratorių prisijungimas (ir nesėkmingi bandymai prisijungti) ir atsijungimas;

11.1.2.3. IS naudotojų, IS naudotojų grupių, IS administratorių teisių naudotis sistemos ir tinklo ištekliais pakeitimai;

11.1.2.4. IS sąsajoje su viešųjų elektroninių ryšių tinklu įvykius, susijusius su įeinančiais ir išeinančiais duomenų srautais;

11.1.2.5. visi IS naudotojų vykdomi veiksmai (duomenų įvedimas, duomenų paieška ir t. t.);

11.1.2.6. audito funkcijos įjungimas / išjungimas;

11.1.2.7. audito įrašų trynimas, kūrimas ar keitimas;

11.1.2.8. IS ir tinklo parametrų, laiko ir (ar) datos pakeitimai;

11.1.2.9. audituojamų įrašų laiko žymos turi būti sinchronizuotos ne mažiau kaip vienos sekundės tikslumu;

11.1.3. audito įrašai įrašomi automatiniu būdu IS veiksmų žurnale, apsaugotame nuo neteisėto jame esančių duomenų naudojimo, keitimo, iškraipymo, sunaikinimo;

11.1.4. draudžiama audito duomenis trinti, keisti, kol nesibaigęs 2 mėn. audito įrašų saugojimo terminas;

11.1.5. audito įrašų duomenys turi būti analizuojami IS administratoriaus ne rečiau kaip kartą per mėnesį, siekiant nustatyti nesankcionuoto poveikio šaltinį, laiką, pakeitimus ar veiksmus IS programinei įrangai ir elektroninei informacijai. Analizuojami:

11.1.5.1. ugniasienės užfiksuoti įvykiai;

11.1.5.2. veiksmai atlikti IS administratorių paskyromis;

11.1.5.3. atlikti IS konfigūraciniai pakeitimai;

11.1.5.4. atlikti pakeitimai apsaugose nuo kenksmingo programinio kodo (pvz. tarnybinės stoties ugniasienės išjungimas);

11.1.5.5. prisijungimai prie audito įrašų;

11.1.5.6. nesėkmingi prisijungimai prie IS;

11.1.6. IS duomenų bazės veiksmų žurnalo duomenys prieinami tik IS administratoriui (skaitytojo teisėmis) ir Saugos įgaliotiniui;

11.1.7. audito duomenys turi būti archyvuojami. Archyve saugomi duomenys turi būti apsaugoti nuo pažeidimo, praradimo, nesankcionuoto pakeitimo ar sunaikinimo;

11.1.8. audito įrašai turi būti saugomi ne tose pačiose IS tarnybinėse stotyse, kur jie yra sukuriami;

11.1.9. dėl įvairių trikdžių nustojus fiksuoti auditui skirtus duomenis, apie tai nedelsiant turi būti informuojamas IS administratorius ir Saugos įgaliotinis.

11.2. saugaus naudojimosi belaidžiu tinklu saugumo priemonės:

11.2.1. leidžiama naudoti tik su Saugos įgaliotiniu suderintus belaidžio tinklo įrenginius, atitinkančius nustatytus reikalavimus;

11.2.2. prie belaidžio tinklo negalima prijungti įrenginių, neatitinkančių Saugos dokumentuose nustatytų saugumo reikalavimų. Apie bandymus prijungti VMKL nevaldomus ar saugumo reikalavimus neatitinkančius įrenginius informuojamas Saugos įgaliotinis;

11.2.3. tikrinami eksploatuojami belaidžiai įrenginiai, Saugos įgaliotiniui pranešama apie neleistinus ar Taisyklių reikalavimų neatitinkančius belaidžius įrenginius;

11.2.4. belaidės prieigos taškai diegiami tik atskirame potinklyje (logiškai atskirtoje kontroliuojamoje zonoje);

11.2.5. prisijungiant prie belaidžio vidinio tinklo naudojamas EAP-TLS raktas, o prie svečiams skirto belaidžio tinklo – WPA2 raktas;

11.29.6. draudžiama belaidėje sąsajoje naudoti SNMP (angl. Simple Network Management Protocol) protokolą tinklo įrenginių valdymui;

11.2.7 draudžiami visi nebūtini valdymo protokolai;

11.2.8. draudžiamas lygiarangis (angl. peer to peer) funkcionalumas;

11.2.9. turi būti išjungti nenaudojami TCP (angl. Transmission Control Protocol) / UDP (angl. User Datagram Protocol) prievadai;

11.2.10. belaidis ryšys turi būti šifruojamas mažiausiai 128 bitų ilgio raktu;

11.2.11. pradedant šifruoti belaidį ryšį, turi būti pakeisti belaidės prieigos stotelės standartiniai gamintojo raktai;

11.2.12. VMKL IS tinklo įrangos ugniasienėje turi būti nustatytas draudimas, kad iš belaidžio elektroninės informacijos perdavimo potinklio nebūtų galima prieiti prie darbinės aplinkos;

11.3. elektroninio pašto saugumo priemonės:

11.3.1. VMKL elektroninio pašto dėžutės kuriamos tik VMKL darbuotojams. Išimtinais atvejais, VMKL elektroninio pašto dėžutės gali būti kuriamos paslaugų teikėjų įgaliotiems asmenims, jų VMKL teikiamoms paslaugoms tinkamai atlikti;

11.3.2. VMKL elektroninio pašto administratoriai kiekvienam VMKL IS naudotojui sukuria elektroninio pašto dėžutę „Pašto dėžutė – <VMKL elektroninio pašto naudotojo vardo pirma raidė ir pavardė>“ (toliau – Pašto dėžutė). Atskiri padaliniai gali turėti bendro naudojimo elektroninio pašto dėžutes;

11.3.3. VMKL elektroninio pašto dėžutės elektroninio pašto adresas sudaromas iš VMKL darbuotojo vardo pirmos raidės ir pavardės, atskirtų tašku arba padalinio pavadinimo ar trumpinio, ženklelio "@" ir elektroninio pašto srities vardo (v.pavardenis@vmkl.lt ar statistika@vmkl.lt).

11.3.4. VMKL elektroninio pašto dėžučių dydis yra ribojamas 1 TB / neribojamas;

11.3.5. naudojamos šifravimo priemonės ryšiui tarp pašto dėžutės naudotojo ir pašto serverio apsaugoti;

11.3.6. turi būti naudojamos apsaugos priemonės nuo nepageidaujamo turinio laiškų;

11.3.7. visi laiškai prieš patenkant į naudotojo pašto dėžutę turi būti skanuojami dėl kenksmingos programinės įrangos ir veikloje nenaudojamų failų tipų;

11.3.8. ištrinti iš elektroninio pašto dėžutės laiškai, pašto serveryje saugomi kol pasibaigs įvykių saugojimo laikas.

11.3.9. VMKL elektroninio pašto naudotojams rekomenduojama įspėti trečiuosius asmenis nesiųsti į VMKL elektroninio pašto dėžutes draudžiamo tipo bylų;

11.3.10. VMKL elektroninio pašto naudotojams draudžiama:

11.3.10.1. VMKL elektroniniu paštu siųsti neužšifruotą viešai neskelbtiną informaciją ne VMKL elektroninio pašto naudotojams, kuriems ji turėtų būti perduodama pagal VMKL ir trečiųjų šalių pasirašytas sutartis;

11.3.10.2. VMKL elektroniniu paštu siųsti VMKL IS naudotojo vardus su slaptažodžiu, išskyrus laikinus slaptažodžius, skirtus vienkartinei prieigos prie IS slaptažodžiui pasikeisti;

11.3.10.3. VMKL elektroniniu paštu 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;

11.3.10.4. naudoti VMKL elektroninį paštą pasipelnymo, politinės reklamos ar kitais savanaudiškais tikslais;

11.3.10.5. skaityti kitų VMKL elektroninio pašto naudotojų elektroninius laiškus be jų sutikimo;

11.3.11. gavęs elektroninį laišką VMKL elektroninio pašto naudotojas turi įvertinti, ar siuntėjas yra žinomas ir ar buvo tikimasi iš tokio siuntėjo gauti elektroninį laišką, o taip pat ar elektroninio laiško tema nekelia įtarimo. Jeigu VMKL elektroninio pašto naudotojui nėra žinomas elektroninio laiško siuntėjas, jo elektroniniu laišku atsiųstos bylos ar nuorodos į nežinomas interneto svetaines kelia įtarimų, draudžiama atversti elektronines bylas ir nuorodas, nes jose gali būti kenksminga programinė įranga. Jeigu VMKL elektroninio pašto naudotojui siuntėjas yra žinomas, bet atsiųsti elektroninio laiško priedai įtartini, būtina elektroniniu paštu ar kitomis ryšio priemonėmis susisiekti su elektroninio laiško siuntėju ir išsiaiškinti, ar tikrai jis siuntė elektroninį laišką su tokiais priedais. VMKL elektroninio pašto naudotojui nerekomenduojama atsakyti į elektroninius laiškus, jeigu kilo abejonių dėl elektroninio laiško siuntėjo tapatybės tikrumo, nes elektroniniame pašte egzistuoja galimybė apsimesti kitu asmeniu;

11.3.12. sprendžiant VMKL informacijos saugumo incidentus, VMKL elektroninio pašto naudotojų gauti ir išsiųsti elektroniniai laiškai ir jų priedai gali būti nagrinėjami tik esant VMKL vadovo raštiškam pavedimui.

11.3.13. jei iškyla grėsmė VMKL IS saugumui, VMKL elektroninio pašto administratorius bet kuriuo metu be išankstinio perspėjimo gali apriboti VMKL elektroninio pašto naudotojo (-ų) arba VMKL viešojo (-ųjų) aplanko (-ų) darbą.

12. IS veikimo užtikrinimas:

12.1. IS vienkartinis neveikimo dėl incidentų laikotarpis negali būti ilgesnis nei 16 val.;

12.2. IS vienkartinis neveikimo dėl profilaktinių darbų, plėtros darbų ir kt. laikotarpis negali būti ilgesnis nei 2 val.;

12.3. IS prieinamumas turi būti užtikrintas ne mažiau kaip 95 proc. laiko visą parą (IS neprieinamumo bendra trukmė per metus valandomis – iki 438 val.).

**III SKYRIUS**

**SAUGUS ELEKTRONINĖS INFORMACIJOS TVARKYMAS**

13. Saugaus elektroninės informacijos keitimo, atnaujinimo, įvedimo ir naikinimo užtikrinimo tvarka:

13.1. elektroninė informacija į IS gali būti įvedama, joje keičiama, atnaujinama ir naikinama tik Taisyklių, Nuostatų, Duomenų saugos nuostatų ir kitų teisės aktų, reglamentuojančių IS veiklą ir elektroninės informacijos tvarkymą, nustatyta tvarka;

13.2. elektroninė informacija gali būti tvarkoma pagal IS naudotojams ir IS administratoriams suteiktas prieigos teises ir tik turint teisėtą tikslą ir pagrindą;

13.3. visi IS naudotojų veiksmai registruojami Taisyklių 11.1 papunktyje nustatyta tvarka;

13.4. IS naudotojui neatliekant jokių veiksmų 15 minučių, IS taikomoji programinė įranga turi užsirakinti, kad toliau naudotis IS galima būtų tik pakartotinai atlikus savo tapatybės nustatymo ir autentiškumo patvirtinimo veiksmus;

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

13.6. IS turi turėti įvestos elektroninės informacijos tikslumo, užbaigtumo, patikimumo tikrinimo ir informavimo apie klaidas priemones.

14. IS elektroninės informacijos atsarginių kopijų darymo ir atkūrimo reikalavimai:

14.1. VMKL IS elektroninės informacijos duomenų bazės atsarginės kopijos daromos ne rečiau kaip vieną kartą per valandą, tuo tarpu IS elektroninės informacijos atsarginės kopijos, apimančios per einamąją dieną įvykusius IS elektroninės informacijos pakeitimus, daromos ne rečiau kaip vieną kartą per einamąją dieną;

14.2. IS elektroninė informacija atsarginėse kopijose saugoma užšifruota (šifravimo raktai saugomi atskirai nuo kopijų) arba imamasi kitų priemonių, neleidžiančių panaudoti kopijas neteisėtai atkurti IS elektroninę informaciją;

14.3. IS administratorius atlieka įdiegtos IS rezervinio kopijavimo ir atkūrimo sistemos, darančios atsargines IS elektroninės informacijos kopijas bei jas archyvuojančios, priežiūrą, esant poreikiui iš duomenų atsarginių kopijų atkuria IS elektroninę informaciją;

14.4. IS elektroninės informacijos atsarginės kopijos turi būti saugomos nedegiose spintose, kitose patalpose nei yra tarnybinė stotis, iš kurios elektroninė informacija buvo nukopijuota, arba kitame pastate;

14.5. patalpos, kuriose saugomos IS elektroninės informacijos atsarginės kopijos, turi būti rakinamos, įrengti gaisro ir apsauginės signalizacijos jutikliai, prijungti prie pastato signalizacijos ir/arba apsaugos tarnybos stebėjimo pulto. Patekti į patalpas gali Saugos įgaliotinis ir IS administratorius bei jų lydimi asmenys;

14.6. IS elektroninės informacijos atkūrimo iš atsarginių kopijų testavimas atliekamas ne rečiau kaip du kartus per metus, atkūrimą iš atsarginių kopijų inicijuoja Saugos įgaliotinis ir/ ar IS administratorius;

14.7. Prarasti, iškraipyti ar sunaikinti IS duomenys atkuriami iš atsarginių duomenų kopijų.

15. Elektroninė informacija perkeliama ir teikiama susijusiems registrams ir (ar) kitoms informacinėms sistemoms ir iš jų gaunama vadovaujantis Nuostatuose nustatyta tvarka ir sąlygomis.

16. Elektroninės informacijos neteisėto kopijavimo, keitimo, naikinimo, perdavimo ar kitokios neteisėtos veiklos (toliau – neteisėta veikla) nustatymo tvarka:

16.1. siekiant nustatyti, ar su IS elektronine informacija nėra vykdoma neteisėta veikla, visi elektroniniuose įvykių žurnaluose saugomi įrašai turi būti analizuojami ne rečiau kaip kartą per savaitę, už įvykių žurnalų analizę atsakingas IS administratorius;

16.2. IS naudotojai, pastebėję Taisyklėse, Duomenų saugos nuostatuose, Taisyklėse, VMKL IS veiklos tęstinumo valdymo plane nustatytų reikalavimų pažeidimų, nusikalstamos veikos požymių, neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos ir 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 pranešti apie tai IS administratoriui, IS tvarkytojo saugos įgaliotiniui arba Informacinių technologijų ir komunikacijos skyriaus darbuotojams;

16.3. IS tvarkytojo saugos įgaliotinis, įtaręs, kad su elektronine informacija, tvarkoma IS, vykdoma neteisėta veikla, inicijuoja elektroninės informacijos saugos ir kibernetinių incidentų valdymo procedūras.

17. IS programinės ir techninės įrangos keitimo, IS pokyčių valdymo tvarka:

17.1. IS pokyčiai inicijavimo priežastys:

17.1.1. IS tobulinimas ir (ar) plėtra atsižvelgiant į pasikeitusius teisės aktų reikalavimus bei sąsajas su kitomis valstybės informacinėmis sistemomis ir registrais;

17.1.2. IS tobulinimas ir (ar) plėtra atsižvelgiant į IS naudotojų ir administratorių poreikius;

17.1.3. elektroninių paslaugų pacientams teikimo tobulinimas ir (ar) plėtra;

17.1.4. IS rizikos įvertinimo metu nustatytos rizikos;

17.1.5. IS informacinių technologijų saugos reikalavimų atitikties vertinimo metu nustatyti trūkumai;

17.1.6. IS elektroninės informacijos saugos incidentas;

17.1.7. pasikartojančios IS veikimo klaidos;

17.1.8. IS infrastruktūros tobulinimas ar jos plėtra;

17.1.9. IS reorganizavimas ar modernizavimas;

17.2. IS pokyčius inicijuoja IS administratorius, IS saugos įgaliotinis ar VMKL padalinio, kuriame kilo poreikis IS pokyčiams, vadovas.

17.3. Pokyčio valdymas ir įgyvendinimas organizuojamas atsižvelgiant į pokyčių kategorijas:

17.3.1. standartinis pokytis – pokytis, kurio įgyvendinimo veiksmai iš anksto yra žinomi ir jie nekelia rizikos kokybiškam IS veikimui;

17.3.2. skubus pokytis – pokytis, skirtas sutrikimams ar problemoms šalinti, kuomet reikia skubos tvarka įvertinti , patvirtinti ir įgyvendinti IS pokyčius;

17.3.3. vystymo pokytis – pokytis, kuriuo yra kuriamos ar modernizuojamos IS funkcijos ir su tuo susiję pokyčio atlikimo veiksmai nėra visiškai aiškūs, o pokyčio įgyvendinimas yra susijęs su tam tikra rizika IS veikimui.

17.4. Skubūs pokyčiai, vystymo pokyčiai ir visi kiti pokyčiai, galintys sutrikdyti ar sustabdyti informacinės sistemos darbą, turi būti suderinti su VMKL vadovu, IS saugos įgaliotiniu ar IS administratoriumi ir vykdomi tik gavus jų raštišką pritarimą.

17.5. Pokyčio įgyvendinimą kontroliuoja IS administratorius: svarsto pokyčius iniciavusių VMKL padalinių pasiūlymus, koordinuoja vystymo pokytį įgyvendinančių tiekėjų veiksmus, teikia pasiūlymus VMKL vadovui, IS saugos įgaliotiniui.

17.6. Pokyčių įgyvendinimo eiga, esant galimybei, registruojama IS priežiūrą vykdančio tiekėjo elektroninėje pagalbos sistemoje.

17.7. Pokyčiai, galintys sutrikdyti ar sustabdyti IS darbą, daryti neigiamą įtaką elektroninės informacijos konfidencialumui, vientisumui ar prieinamumui, turi būti patikrinti testavimui skirtoje aplinkoje, kurioje nėra konfidencialių ir asmens duomenų ir kuri atskirta nuo IS darbinės aplinkos. Pokyčiai darbinėje aplinkoje gali būti vykdomi tik išimtiniais atvejais, kai dėl techninių, programinių ar kitų priežasčių (pvz., veiklos atkūrimas ir kitos avarinės situacijos ir pan.) pokyčių nėra galimybės patikrinti testavimui skirtoje IS aplinkoje.

17.8. Nustačius, kad pokyčių testavimo testavimui skirtoje aplinkoje rezultatas atitinka laukiamus rezultatus, pokyčiai gali būti atliekami darbinėje IS aplinkoje.

17.9. IS administratorius arba pokytį įgyvendinantis tiekėjas turi informuoti IS naudotojus, susijusius IS tvarkytojus, kitus suinteresuotus asmenis apie pokyčius, kurių įgyvendinimo metu galimi IS darbo sutrikimai. Apie pokyčius turi būti informuojama pokyčius įgyvendinančio subjekto IS taikomosiose programose ar kitomis priemonėmis (pvz., raštu, elektroniniu paštu ir pan.) ne vėliau kaip prieš vieną darbo dieną iki planuojamo pokyčio įgyvendinimo pradžios. Šio punkto nuostatų gali būti nesilaikoma, jeigu įgyvendinami skubūs pokyčiai.

17.10. Įgyvendinus pokytį, IS administratorius ir pokyčio iniciatorius turi patikrinti (peržiūrėti) IS sąranką ir IS būsenos rodiklius, palyginti ir pagal kompetenciją įvertinti, ar pokytis atitinka planuojamus rezultatus. Sudėtingiems ir specifinių pokyčių rezultatams įvertinti gali būti pasitelkti ir kiti VMKL ar IS priežiūros paslaugų teikėjo kompetentingi specialistai.

17.11. Jei pokytis atitinka planuotus rezultatus, IS administratorius arba IS priežiūros paslaugų teikėjas turi atnaujinti IS sąrankos aprašus ir IS naudotojų instrukcijas.

17.12. Jei siekiant įgyvendinti vystymo pokytį turi būti keičiami IS nuostatai ar kiti IS veiklą reglamentuojantys teisės aktai, jų pakeitimo projektą rengia pokyčio iniciatorius ar IS administratorius.

18. Nešiojamųjų kompiuterių ir kitų mobiliųjų įrenginių (toliau kartu – mobilieji įrenginiai) naudojimo tvarka:

18.1. leidžiama naudoti tik su VMKL IS saugumo įgaliotiniu suderintus mobiliuosius įrenginius, atitinkančius VMKL IS techninei įrangai keliamus kibernetinio saugumo reikalavimus;

18.2. IS administratorius turi turėti visas teises valdyti mobiliuosius įrenginius ir juose įdiegtą programinę įrangą, tikrinti eksploatuojamus mobiliuosius įrenginius ir IS saugumo įgaliotiniui pranešti apie neleistinus ar techninių saugumo reikalavimų neatitinkančius mobiliuosius įrenginius;

18.3. turi būti naudojamos priemonės, kurios automatiškai apribotų neleistinus ar saugumo reikalavimų neatitinkančius mobiliuosius įrenginius ar informuotų IS administratorių apie neleistinos mobiliosios įrangos prijungimą prie VMKL IS;

18.4. mobiliuosiuose įrenginiuose privalo būti naudojamos centralizuotai valdomos ir atnaujinamos kenkimo programinės įrangos aptikimo, užkardymo ir stebėjimo realiuoju laiku priemonės;

18.5. mobiliuosiuose įrenginiuose turi būti naudojamos vykdomojo kodo (angl. Executable code) kontrolės priemonės, automatiškai apribojančios neleistino vykdomojo kodo naudojimą ar informuojančios IS administratorių apie neleistino vykdomojo kodo naudojimą;

18.6. mobilieji įrenginiai, kuriais naršoma internete, privalo būti apsaugoti nuo judriųjų programų (angl. Mobile code) keliamų grėsmių įdiegiant operacinės sistemos ir kitos naudojamos programinės įrangos gamintojų rekomenduojami atnaujinimai;

18.7. mobiliuosiuose įrenginiuose ir išorinėse kompiuterinėse laikmenose esanti elektroninė informacija privalo būti šifruojama, turi būti užtikrinama laikmenų fizinė apsauga;

18.8. mobiliuosiuose įrenginiuose privalo būti įdiegtos priemonės, leisiančios nuotoliniu būdu neatkuriamai ištrinti duomenis;

18.9. mobilusis įrenginys, kuriuo nesinaudojama 5 minutes, turi automatiškai užsirakinti;

18.10. prie mobiliųjų įrenginių draudžiama prijungti kokius nors kitus toms sistemoms nepriklausančius įrenginius. VMKL IS valdytojo sprendimu prie mobiliųjų įrenginių gali būti jungiami kiti įrenginiai. Tokiu atveju IS administratoriaus parengia ir su IS saugos įgaliotiniu suderina leistinų jungti įrenginių sąrašą;

18.11. mobiliųjų įrenginių naudojimas ne VMKL patalpose:

18.11.1. mobilieji įrenginiai naudojami tik tarnybinėms funkcijoms vykdyti;

18.11.2. IS naudotojai mobiliųjų įrenginių negali prijungti prie nesaugių, nešifruotų viešųjų interneto prieigos taškų;

18.11.3. IS naudotojai turi užtikrinti mobiliųjų įrenginio fizinį saugumą, dirbdami turi įsitikinti, kad nėra stebimi (stebimas ekranas) pašalinių asmenų, negali palikti mobiliųjų įrenginių be priežiūros;

18.12. jeigu prie IS jungiamasi per IS infrastruktūroje esančius tarpinius įrenginius:

18.12.1. duomenys perduodami tarp mobiliojo įrenginio ir VMKL IS, turi būti šifruojami taikant VPN technologiją;

18.12.2. patvirtinant tapatumą mobiliajame įrenginyje ar jo taikomojoje programinėje įrangoje uždrausta automatiškai išsaugoti slaptažodį;

18.13. jeigu prie IS iš mobiliųjų įrenginių jungiamasi tiesiogiai, turi būti įgyvendinti šie reikalavimai:

18.13.1. mobiliesiems įrenginiams, naudojamiems IS valdytojo ar IS tvarkytojo patalpose, esantiems vidiniame IS tvarkytojo kompiuterių tinkle, taikomi tokie patys elektroninės informacijos saugos ir kibernetinio saugumo reikalavimai kaip ir stacionariesiems kompiuteriams;

19. Metodai, kuriais leidžiama užtikrinti saugų elektroninės informacijos teikimą ir (ar) gavimą:

19.1. elektroninei informacijai teikti ir (ar) gauti gali būti naudojamas Saugus valstybinis duomenų perdavimo tinklas;

**IV SKYRIUS**

**REIKALAVIMAI, KELIAMI INFORMACINEI SISTEMAI FUNKCIONUOTI REIKALINGOMS PASLAUGOMS IR JŲ TEIKĖJAMS**

20. IS funkcionuoti reikalingų paslaugų, darbų ir (ar) įrangos tiekėjas (toliau – tiekėjas) turi atitikti IS veiklą reglamentuojančių teisės aktų, standartų, Taisyklių reikalavimus ir paslaugų teikimo, darbų atlikimo ar įrangos tiekimo pirkimo dokumentuose iš anksto nustatomus tiekėjo kompetencijos, patirties, teikiamų paslaugų, atliekamų darbų ar tiekiamos įrangos reikalavimus.

21. Perkant paslaugas, darbus ar įrangą, susijusius su IS, jos projektavimu, kūrimu, diegimu, modernizavimu ir kibernetinio saugumo užtikrinimu, iš anksto pirkimo dokumentuose turi būti nustatoma, kad tiekėjas užtikrina atitiktį Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše, nustatytiems reikalavimams. Perkamos paslaugos, darbai ar įranga, susiję su IS, turi atitikti teisės aktų ir standartų, kuriais vadovaujamasi užtikrinant IS elektroninės informacijos saugą ir kibernetinį saugumą, reikalavimus, kurie iš anksto nustatomi paslaugų teikimo, darbų atlikimo ar įrangos tiekimo pirkimo dokumentuose.

22. Tiekėjas, vykdydamas sutartinius įsipareigojimus, turi įgyvendinti tinkamas organizacines ir technines priemones, skirtas IS ir jose tvarkomai elektroninei informacijai apsaugoti nuo atsitiktinio ar neteisėto sunaikinimo, pakeitimo, atskleidimo, taip pat nuo bet kokio kito neteisėto tvarkymo.

23. Tiekėjui prieiga prie IS 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. IS saugos įgaliotinis turi supažindinti tiekėją su suteiktos prieigos IS saugos ir kibernetinio saugumo reikalavimais ir sąlygomis. IS saugos administratorius yra atsakingas už prieigos prie IS tiekėjui suteikimą ir panaikinimą pasirašius sutartį, pasibaigus sutarties su tiekėju galiojimo terminui ar kitais sutartyje nurodytais prieigos prie IS panaikinimo atvejais.

24. Tiekėjui suteikiamas tik toks prieigos prie IS lygmuo, kuris yra būtinas sutartyje nustatytiems įsipareigojimams vykdyti. Tiekėjo paskirti specialistai turi pasirašyti konfidencialumo pasižadėjimus.

25. Iškilus poreikiui, siekiant įsitikinti, ar tinkamai vykdoma sutartis, laikomasi elektroninės informacijos saugos ir kibernetinio saugumo reikalavimų, IS tvarkytojas turi teisę atlikti tiekėjo teikiamų paslaugų stebėseną ir auditą, suteikti galimybę atlikti auditą trečiosioms šalims.

26. Tiekėjas privalo nedelsdamas informuoti IS tvarkytoją apie sutarties vykdymo metu pastebėtus elektroninės informacijos saugos ar kibernetinius incidentus, pastebėtas neveikiančias arba netinkamai veikiančias elektroninės informacijos saugos ir (ar) kibernetinio saugumo užtikrinimo priemones, elektroninės informacijos saugos ir (ar) kibernetinio saugumo reikalavimų nesilaikymą, nusikalstamos veikos požymius, saugumo spragas, pažeidžiamumus, kitus svarbius saugai įvykius.

27. IS tvarkytojas su interneto paslaugų teikėju (-ais) turi būti sudaręs sutartis dėl apsaugos nuo IS elektroninių paslaugų trikdymo taikymo (angl. *denial of service*), reagavimo į elektroninės informacijos saugos ir kibernetinius incidentus įprastomis darbo valandomis ir po darbo valandų, nepertraukiamo interneto paslaugos teikimo ir interneto paslaugos sutrikimų registravimo 24 valandas per parą, 7 dienas per savaitę.

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_