VALSTYBĖS ĮMONĖS ŽEMĖS ŪKIO DUOMENŲ CENTRO INFORMACIJOS SAUGUMO POLITIKA

I SKYRIUS
BENDROSIOS NUOSTATOS

1. Valstybės įmonės Žemės ūkio duomenų centro informacijos saugumo politika (toliau – Politika) yra pagrindinis dokumentas, nustatantis esminius valstybės įmonės Žemės ūkio duomenų centro (toliau – ŽŪDC) informacijos saugumo užtikrinimo ir valdymo principus.

2. Politikos tikslas – pateikti ŽŪDC vadovybės požiūrį į informacijos saugumo valdymą ir nustatyti informacijos saugumo tikslus bei principus.

3. Politika yra privaloma visiems ŽŪDC darbuotojams, kitiems fiziniams ir juridiniams asmenims bei jų atstovams, kuriems teisės aktų ir (arba) sutartinių santykių pagrindu yra suteikta prieiga prie ŽŪDC informacinių išteklių teisės aktuose ar sutartyse numatytoms funkcijoms (teisėms) atlikti.

4. Politika parengta vadovaujantis ISO/IEC 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga“ (toliau – ISO 27001) reikalavimais.

5. Politikoje vartojamos sąvokos:

5.1. **darbuotojas** – ŽŪDC darbuotojas, dirbantis pagal darbo sutartį ar sutartinius įsipareigojimus;

5.2. **informacija** – visa ŽŪDC gaunama, tvarkoma, kuriama, valdoma ir naudojama žodinė, rašytinė ir elektroninė informacija (dokumentai, ŽŪDC tvarkomų informacinių sistemų ir registrų / kadastrų, vidaus administravimo sistemų, duomenų bazių duomenys ir pan.);

5.3. **informacijos saugos incidentas** – vienas ar daugiau nepageidaujamų ar netikėtų įvykių, turinčių didelę tikimybę pakenkti ŽŪDC veiklai ir keliančių grėsmę informacijos saugumui;

5.4. **informacijos saugos įvykis** – įvykis, susijęs su informacija ar informacijos apdorojimo priemone, rodantis galimą Politikos ar kitų saugumo reikalavimų spragą ar apsaugos priemonių trikdį arba anksčiau nenumatytos situacijos, turinčios poveikį (teigiamą ar neigiamą) saugumui užtikrinti, atsiradimą;

5.5. **informaciniai ištekliai** – ŽŪDC veiklos procesai ir informacija, kurią valdo ir tvarko ŽŪDC, atlikdama teisės aktuose nustatytas funkcijas, ir informacinių technologijų priemonės, naudojamos informacijai tvarkyti;

5.6. **informacinio ištekliaus savininkas** – registro / kadastro, valstybės informacinės sistemos duomenų valdymo įgaliotinis arba ŽŪDC struktūrinio padalinio vadovas ar kitas darbuotojas, atsakingas už informacinį išteklių, valdomą ar tvarkomą informaciją ir informacinio ištekliaus informacijos saugą, prisiimantis riziką už informacinį išteklių;

5.7. **informacijos saugumas** – informacijos konfidencialumo, vientisumo ir prieinamumo išsaugojimas; taip pat informacijos saugumas apima tokias informacijos savybes kaip informacijos autentiškumas, atskaitingumas, neišsižadėjimas ir patikimumas;

5.8. **informacijos saugumo valdymo sistema (ISVS)** – rizikų valdymu pagrįsta ŽŪDC vadybos sistemos dalis, kuria siekiama sukurti, įgyvendinti, valdyti, stebėti, vertinti, prižiūrėti ir gerinti informacijos saugumą;

5.9. **išorinis naudotojas** – išorinių organizacijų atstovas, rangovų atstovas, kitas fizinis arba juridinis asmuo, dirbantis / veikiantis pagal informacijos arba paslaugų teikimo sutartį, kuriam sutarties ar galiojančių teisės aktų pagrindu yra suteikta prieiga prie informacijos, informacinių sistemų ir registrų / kadastrų, informacijos apdorojimo priemonių ir (arba) duomenų bazių sutartyje ar galiojančiuose teisės aktuose numatytoms funkcijoms atlikti;

5.10. **konfidencialumas** – informacijos savybė, reiškianti, kad su informacija gali susipažinti tik įgalioti asmenys;

5.11. **konfidencialumo pasižadėjimas** – naudotojų raštiškas pasižadėjimas neteikti tretiesiems asmenims informacijos, kurios atskleidimas gali pažeisti ŽŪDC interesus ir gali turėti įtakos ŽŪDC informacijos saugumui;

5.12. **naudotojas** – vidinis ir išorinis naudotojas;

5.13. **pasiekiamumas (prieinamumas)** – informacijos savybė, reiškianti, kad informacija gali būti tvarkoma reikiamu metu;

5.14. **suinteresuotosios šalys** – fiziniai ir juridiniai asmenys, nustatantys informacijos saugumo reikalavimus ar privalantys laikytis ŽŪDC nustatytų informacijos saugumo reikalavimų, t. y. Lietuvos Respublikos žemės ūkio ministerija, Lietuvos Respublikos aplinkos ministerija, esami ir potencialūs užsakovai, darbuotojai, tiekėjai, rangovai, ŽŪDC valdybos nariai, verslo subjektai, socialiniai partneriai, valstybės institucijos ir kitos įstaigos;

5.15. **tretieji asmenys** – visi fiziniai arba juridiniai asmenys arba jų grupės, neturintys teisės susipažinti su ŽŪDC informacija ar jos tvarkyti, išskyrus naudotojus;

5.16. **informacijos saugumo projektų vadovas (toliau – ISPV)** – darbuotojas, atsakingas už pasiūlymų teikimą ŽŪDC generaliniam direktoriui Politikos formavimo proceso metu, jos įgyvendinimo kontrolę, informacijos klasifikavimą, kasmetinį (jei reikia – neeilinį) rizikos vertinimą, įskaitant kasmetinį informacijos saugumo priemonių testavimą, ŽŪDC darbuotojų mokymą, instruktavimą ir priežiūrą informacijos saugumo klausimais;

5.17. **vidinis naudotojas** – darbuotojas, kuriam yra suteikta prieiga prie informacijos, registrų / kadastrų, informacinių sistemų ir (arba) duomenų bazių darbo sutartyje, struktūrinio padalinio nuostatuose, pareigybės aprašyme / pareiginėje instrukcijoje ir kituose ŽŪDC teisės aktuose numatytoms funkcijoms atlikti;

5.18. **vientisumas** – informacijos savybė, reiškianti, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

6. Kitos Politikoje vartojamos sąvokos atitinka sąvokas, vartojamas ISO 27001.

II SKYRIUS
INFORMACIJOS SAUGUMO VALDYMO SISTEMOS TIKSLAI, APIMTIS IR VADOVYBĖS ĮSIPAREIGOJIMAI. REGLAMENTUOJANTYS DOKUMENTAI

7. Informacija yra viena vertingiausių ŽŪDC turto dalių, todėl jos praradimas, neteisėtas pakeitimas, atskleidimas ar informacijos apdorojimo nutraukimas gali sukelti ŽŪDC veiklos sutrikimų, padaryti žalos ŽŪDC, kitiems fiziniams ir juridiniams asmenims. Atsižvelgiant į tai, ŽŪDC yra keliami ir nustatomi reikalavimai informacijos saugumui.

8. ŽŪDC informacijos saugumo reikalavimų įgyvendinimas užtikrinamas ir valdomas nuosekliai planuojant, įgyvendinant, vertinant ir tobulinant informacijos saugumo valdymo sistemą (toliau – ISVS), vadovaujantis ISO 27001 ir Lietuvos Respublikos teisės aktų reikalavimais. Su informacijos saugumu susijusių aktualių teisės aktų sąrašas yra žinomas ŽŪDC darbuotojams, periodiškai atnaujinamas ir prieinamas darbuotojams bei suinteresuotosioms šalims.

9. ISVS tikslai:

9.1. apsaugoti visą informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos ŽŪDC vykdomai veiklai ir įvaizdžiui;

9.2. įgyvendinti Lietuvos Respublikos teisės aktuose ir ISO 27001 reglamentuotų informacijos saugumo reikalavimų laikymąsi;

9.3. užtikrinti reikiamų informacijos saugumo valdymo priemonių įgyvendinimą;

9.4. išvengti incidentų, susijusių su informacijos saugumo pažeidimais, galinčiais sutrikdyti ŽŪDC veiklą, arba sumažinti tokių incidentų galimą poveikį.

10. Veiksmingos ISVS įdiegimas ir ISO 27001 sertifikavimas padeda įmonei:

10.1. stiprinti pozicijas rinkoje įgyjant konkurencinį pranašumą teikiant pasiūlymus, dalyvaujant konkursuose ir auginant įmonės reputaciją;

10.2. didinti suinteresuotųjų šalių pasitikėjimą, demonstruojant įsipareigojimą užtikrinti informacijos saugumą ir duomenų apsaugą;

10.3. valdyti rizikas, užtikrinant, kad būtų apsaugotas ŽŪDC turtas, vertingi duomenys, intelektinė nuosavybė ir veiklos vientisumas;

10.4. greitai reaguoti į galimus informacijos saugos incidentus, sumažinant veiklos sutrikimus ir finansines pasekmes;

10.5. laikytis nacionalinių ir tarptautinių reguliavimo reikalavimų, susijusių su informacijos saugumu ir duomenų apsauga.

11. Siekdama ISVS tikslų ŽŪDC vadovybė įsipareigoja:

11.1. siekti, kad Politika ir tikslai būtų suderinti su ŽŪDC strateginiais bei veiklos tikslais;

11.2. skirti reikiamą dėmesį bei resursus nustatytų ISVS tikslų įgyvendinimui;

11.3. nuolatos tobulinti / gerinti ISVS periodiškai peržiūrint ISVS tikslus;

11.4. paskirti už informacijos saugumą atsakingą darbuotoją / darbuotojus, kuris / kurie būtų atsakingas / atsakingi už Politikos ir joje iškeltų tikslų įgyvendinimą ir priežiūrą;

11.5. užtikrinti ISVS reikalavimų integravimą į ŽŪDC procesus. Patvirtinti ISVS, Politikos įgyvendinimui reikalingus dokumentus, tvarkas, procedūras ir supažindinti su jais visus ŽŪDC darbuotojus bei suinteresuotąsias šalis;

11.6. užtikrinti reikiamą darbuotojų kompetenciją – sudaryti sąlygas tobulinti žinias ir kelti savo kvalifikaciją informacijos saugumo srityje;

11.7. nustatyti pamatuojamus tikslus nurodant juose įsipareigojimus informacijos saugumui, ir kasmet vertinti nustatytų tikslų įgyvendinimą bei, atsižvelgiant į pasiektus rezultatus, peržiūrėti ISVS, Politikos aktualumą bei tinkamumą ir skatinti nuolatinį tobulėjimą;

11.8. numatyti atsakomybę už informacijos saugumo reikalavimų nesilaikymą.

12. ISVS taikoma ŽŪDC sertifikavimo srityje:

12.1. visuose ŽŪDC veiklos procesuose ir visiems struktūriniams padaliniams;

12.2. visai informacijai (nepriklausomai nuo jos formos ir saugojimo būdo);

12.3. visiems ŽŪDC informaciniams ištekliams ir technologijoms, taip pat IT infrastruktūrai, programoms, duomenims, procesams, resursams bei paslaugoms;

12.4. vidiniams ir išoriniams naudotojams;

12.5. visiems trečiųjų šalių paslaugų tiekėjams, turintiems prieigą prie ŽŪDC informacinių išteklių, IT sistemų ar kurie apdoroja ŽŪDC duomenis.

13. ŽŪDC ISVS sertifikavimo sritis: Informacinių paslaugų teikimas, registrų ir informacinių sistemų kūrimas ir tvarkymas; Žemės sklypų kadastrinių matavimų ir kitų nekilnojamųjų daiktų kadastro duomenų nustatymas, geodezijos, inžinerinių tinklų ir topografijos darbų veikla, žemės reformos, žemėtvarkos ir teritorijų planavimo dokumentų rengimas, detaliųjų ir specialiųjų planų rengimas ir kiti, su tuo susiję darbai, specialiųjų žemės sąlygų bei servitutų nustatymo planų rengimo, dirvožemio, apleistų žemių tvarkymo, melioracijos darbų pardavimo vykdymas, taip pat kitos sritys, kurios sertifikuojamos / sertifikuotos Lietuvos standarte ISO/IEC 27001 nustatyta tvarka.

14. Įgyvendinant ISVS yra siekiama tokių informacijos saugumo tikslų:

14.1. užtikrinti ir valdyti informacijos saugumą, atsižvelgiant į ŽŪDC veiklos (strateginius) tikslus;

14.2. užtikrinti ir valdyti atitikimą išoriniams ir vidiniams informacijos saugumo reikalavimams, atliekant periodinį atitikties vertinimą ir šalinant nustatytus trūkumus;

14.3. užtikrinti informacijos saugumo pažeidimų sprendimą, jų priežasčių nustatymą ir pašalinimą, įgyvendinant informacijos saugos incidentų valdymo procesą;

14.4. užtikrinti tinkamą informacijos saugumo ir apdorojimo priemonių parinkimą ir įgyvendinimą, atliekant kasmetinį rizikos vertinimą ir įgyvendinant rizikos valdymo planą;

14.5. užtikrinti taikomų informacijos saugumo priemonių veiksmingumą;

14.6. užtikrinti veiklos tęstinumo valdymo / atstatymo planų tinkamumą, atliekant jų periodinius peržiūrą ir testavimą.

15. Informacijos saugumo tikslų įgyvendinimas matuojamas kokybės rodiklių matavimo proceso metu. Informacijos saugumo tikslų įgyvendinimo rezultatai gaunami, vertinant ISVS ir priemonių veiksmingumą, o aptariami ISVS vadybos vertinamosios analizės metu.

16. Politiką reglamentuojantys dokumentai:

16.1. ISO 27001.

16.2. BDAR – Bendrasis duomenų apsaugos reglamentas (ES) 2016/679.

16.3. Teisinių, reguliavimo, sutartinių ir kitų reikalavimų sąrašas.

III SKYRIUS
INFORMACIJOS SAUGUMO VALDYMO SISTEMOS VAIDMENYS IR ATSAKOMYBĖS

17. ŽŪDC informacijos saugumo valdymą organizuoja:

17.1. Valdyba;

17.2. ŽŪDC generalinis direktorius (angl. *Chief Executive Officer, CEO*);

17.3. Informacinių technologijų priežiūros ir projektų komitetas (jeigu jis yra sudaromas) (toliau – Komitetas);

17.4. ISPV (angl. *Chief Information Security Officer, CISO*);

17.5. Informacinių technologijų departamento (toliau – ITD) direktorius (angl. *Chief Information Officer, CIO*);

17.6. Duomenų apsaugos pareigūnas (toliau – DAP, angl. *Data Protection Officer, DPO*);

17.7. ŽŪDC informacinių išteklių duomenų valdymo įgaliotiniai (savininkai);

17.8. ŽŪDC informacinių išteklių saugos įgaliotiniai ir administratoriai;

17.9. ISVS auditoriaus funkcijas vykdantis darbuotojas arba paslaugos teikėjas;

17.10. Trečiosios šalys (tiekėjai, partneriai);

17.11. Visi ŽŪDC darbuotojai.

18. Valdybos atsakomybė informacijos saugumo srityje:

18.1. prižiūri Rizikos valdymo plano sudarymą ir įgyvendinimą;

18.2. skiria resursus (biudžetą) Rizikų valdymo plano priemonių (kontrolių) įgyvendinimui;

18.3. prižiūri Rizikos valdymo priemonių įgyvendinimą.

19. ŽŪDC generalinio direktoriaus atsakomybė informacijos saugumo srityje:

19.1. formuoti ir tvirtinti Politiką, ją reglamentuojančius ir su ja susijusius ŽŪDC teisės aktus;

19.2. tvirtinti informacijos saugumo tikslus ir užtikrinti jų atitikimą ŽŪDC veiklos tikslams ir informacijos saugumo reikalavimams;

19.3. tvirtinti informacijos saugumo rizikos vertinimo metodiką ir rezultatus;

19.4. užtikrinti informacijos saugumui įgyvendinti reikalingų finansinių, žmogiškųjų ir technologinių išteklių skyrimą;

19.5. paskirstyti atsakomybę už informacijos saugumą;

19.6. skatinti nustatytų informacijos saugumo reikalavimų laikymąsi;

19.7. užtikrinti nuolatinį ISVS tobulinimą.

20. Komitetas gali būti sudaromas ŽŪDC generalinio direktoriaus sprendimu. Komitetas nagrinėja ir svarsto klausimus, susijusius su informacinių išteklių sauga,

informacinių technologijų naudojimu ŽŪDC, informacijos saugos incidentais ir rizikos vertinimu. Komiteto darbo principai numatomi Komiteto darbo reglamente.

21. ISPV pareigos informacijos saugumo srityje:

21.1. prižiūrėti ISVS kūrimą, įgyvendinimą ir priežiūrą;

21.2. rekomenduoti informacijos saugumo procedūrų atnaujinimus, atsižvelgiant į rizikas ir besikeičiančius veiklos poreikius;

21.3. pranešti apie ISVS veikimą ir incidentus aukščiausiajai vadovybei (Valdybai ir ŽŪDC generaliniam direktoriui);

21.4. užtikrinti, kad būtų laikomasi Politikos, procedūrų ir standartų;

21.5. koordinuoti ISVS auditus;

21.6. gauti naujausią informaciją apie atitinkamus įstatymus, reglamentus ir standartus;

21.7. nustatyti ir įvertinti informacijos saugumo rizikas;

21.8. siūlyti rizikos valdymo, mažinimo galimybes;

21.9. nuolat stebėti ir peržiūrėti riziką;

21.10. užtikrinti, kad rizikos vertinimai būtų atliekami periodiškai.

22. ITD direktoriaus pareigos informacijos saugumo srityje:

22.1. įgyvendinti ir diegti suplanuotas ISVS politikas, procedūras bei techninius IT saugos komponentus;

22.2. valdyti IT saugumo incidentus bei išmoktas pamokas;

22.3. valdyti IT saugos techninę riziką;

22.4. valdyti kasdienines informacijos saugumo operacijas bei technologijas, įskaitant grėsmių, anomalijų ir pažeidžiamumų stebėjimą bei saugos pataisų diegimą;

22.5. valdyti atsarginių kopijų kūrimo ir veiklos atkūrimo procedūras;

22.6. pranešti apie su IT sauga susijusius veiklos rezultatus;

22.7. užtikrinti atitinkamų IT standartų ir reglamentų laikymąsi, kiek tai susiję su IT naudojimu, pvz., BDAR, ISO 27001.

23. DAP pareigos informacijos saugumo srityje:

23.1. padėti ŽŪDC tinkamai įgyvendinti BDAR reikalavimus ir užtikrinti atitiktį tiek BDAR, tiek ir kitiems asmens duomenų tinkamą tvarkymą ir apsaugą reglamentuojantiems teisės aktams;

23.2. glaudžiai bendradarbiauti su ISPV visais klausimais, susijusiais su asmens duomenų saugumo pažeidimais, kurie kartu laikomi ir informacijos saugos įvykiais ar informacijos saugos incidentais;

23.3. ŽŪDC reglamentuota tvarka nustatyti poveikio asmens duomenų apsaugai vertinimo poreikį, organizuoti ir atlikti poveikio asmens duomenų apsaugai vertinimą, kurio metu įvertinamos ir susijusios rizikos bei galimi informacijos konfidencialumo, vientisumo ir prieinamumo aspektai (galimi šių aspektų pažeidimai).

24. ISVS auditoriaus pareigos informacijos saugumo srityje:

24.1. reguliariai atlikti ISVS vidaus auditą;

24.2. pateikti objektyvių įžvalgų apie tai, kaip ISVS atitinka ISO 27001 ir Politiką;

24.3. remiantis audito metu nustatytais faktais, rekomenduoti taisomuosius veiksmus;

24.4. pranešti apie audito metu nustatytus faktus ISPV.

25. Trečiųjų šalių pareigos informacijos saugumo srityje:

25.1. laikytis sutartyse ir susitarimuose nustatytų informacijos saugumo reikalavimų;

25.2. užtikrinti, kad jų pačių saugumo praktika nekeltų pavojaus ŽŪDC informacijai ir turtui;

25.3. pranešti apie visas saugos problemas ar pažeidimus, kurie gali turėti įtakos ŽŪDC.

26. Visų ŽŪDC darbuotojų pareigos informacijos saugumo srityje:

26.1. laikytis ŽŪDC Politikos, susijusių išorinių ir ŽŪDC teisės aktų, kitų dokumentų (pvz., sutarčių), reglamentuojančių / nustatančių informacijos saugumą, reikalavimų;

26.2. nedelsiant pranešti apie pastebėtus galimus ar įvykusius informacijos saugos įvykius ir incidentus el. paštu cert@zudc.lt;

26.3. nedelsiant pranešti apie galimus ar jau įvykusius asmens duomenų saugumo pažeidimus el. paštu duomenuapsauga@zudc.lt;

26.4. dalyvauti privalomuose informacijos saugumo mokymuose;

26.5. atsakingai ir saugiai naudotis IT sistemomis ir duomenimis, informacinius išteklius naudoti tik su darbo / sutartiniais santykiais susijusiais tikslais ir tik suteiktų įgaliojimų ribose, išskyrus jeigu kitaip reglamentuota susijusiuose ŽŪDC teisės aktuose;

26.6. pasirašyti Konfidencialumo pasižadėjimą (Politikos priedas) ir laikytis visų šio pasižadėjimo reikalavimų ir nuostatų;

27. ŽŪDC informacinių išteklių duomenų valdymo įgaliotinių (savininkų), saugos įgaliotinių ir administratorių funkcijos ir atsakomybė informacijos saugumo srityje nustatytos Lietuvos Respublikos teisės aktuose ir ŽŪDC teisės aktuose.

IV SKYRIUS
INFORMACIJOS SAUGUMO RIZIKOS VALDYMAS

28. Informacijos saugumo valdymas ŽŪDC yra pagrįstas rizikos valdymu.

29. ŽŪDC informacijos saugumo rizika vertinama ne rečiau kaip vieną kartą per metus pagal Rizikos valdymo tvarkos aprašą.

30. Rizikos vertinimą atlieka ISPV ir (arba) išorės paslaugos teikėjas.

31. Pagrindinės ISPV pareigos atliekant rizikos vertinimą:

31.1. nustatyti ir įvertinti informacijos saugumo rizikas;

31.2. nuolat stebėti ir peržiūrėti šias rizikas;

31.3. pasiūlyti rizikos valdymo, mažinimo galimybes;

31.4. stebėti rizikos mažinimo priemonių įgyvendinimą;

31.5. užtikrinti, kad rizikos vertinimai būtų atliekami periodiškai.

32. Atsižvelgiant į informacijos saugumo rizikos vertinimo rezultatus parenkamos tinkamos, keliamai rizikai proporcingos, informacijos saugumo valdymo priemonės.

33. Informacijai apsaugoti yra taikomos fizinės, administracinės ir techninės apsaugos priemonės, aprašytos ŽŪDC teisės aktuose.

V SKYRIUS
PAGRINDINIAI INFORMACIJOS SAUGUMO UŽTIKRINIMO VALDYMO REIKALAVIMAI

34. Įgyvendinant ISVS tikslus ir siekiant užtikrinti informacinių išteklių saugą yra nustatomi šie pagrindiniai bendrieji reikalavimai:

34.1. informacijos saugumo užtikrinimo reikalavimai, nustatyti Politikoje ir kituose informacijos saugumą reglamentuojančiuose ŽŪDC teisės aktuose, taikomi visiems ŽŪDC informaciniams ištekliams, nepriklausomai nuo to, kur jie yra, kokioje formoje saugomi, kokios technologijos naudojamos jiems apdoroti ir kokie darbuotojai juos tvarko bei apdoroja;

34.2. visi informaciniai ištekliai turi būti identifikuoti, žinomi ir paskirti informacinių išteklių savininkai. ŽŪDC informacinių išteklių sąrašą sudaro ir periodiškai atnaujina ISPV. Informacinių išteklių savininkai yra atsakingi už priskirtų informacinių išteklių saugą;

34.3. informaciniai ištekliai turi būti apsaugoti nuo neautorizuotos fizinės prieigos, sugadinimo ar kitokio pakenkimo;

34.4. ŽŪDC informaciniai ištekliai turi būti apsaugoti nuo galimų rizikų;

34.5. suteikiant prieigą prie ŽŪDC informacinių išteklių trečiosioms šalims, sutartyse privalo būti įtraukiami konfidencialumo reikalavimai ir informacijos saugumo reikalavimai bei numatyta atsakomybė už šių reikalavimų nevykdymą. Pasibaigus sutartiniams santykiams visa trečiosios šalies turima ŽŪDC informacija, kuri svarbi ŽŪDC tolesnei veiklai, turi būti perduota ŽŪDC;

34.6. kandidatai į pareigas ŽŪDC turi būti patikrinti taip kaip numatyta Lietuvos Respublikos darbo kodekse ir kituose teisės aktuose. Darbuotojų pareigos, įsipareigojimai ir atsakomybė turi būti apibrėžti ir dokumentuoti. Atleidžiamas iš ŽŪDC darbuotojas turi grąžinti visą jam darbo reikmėms suteiktą ŽŪDC turtą ir informaciją, kaip nustatyta ŽŪDC teisės aktuose;

34.7. turi būti periodiškai organizuojami vidinių naudotojų mokymai informacijos saugumo klausimais.

34.8. prieiga prie informacinių išteklių valdoma atsižvelgiant į veiklos ir informacijos saugumo reikalavimus, prieigos teisės naudotojams suteikiamos autorizuotai ŽŪDC teisės aktuose nustatyta tvarka;

34.9. naudotojams turi būti suteikiama prieiga ŽŪDC teisės aktuose nustatyta tvarka tik prie tų tinklų ir tinklo paslaugų, kuriais (kuriomis) naudotis jiems buvo konkrečiai suteikta teisė;

34.10. informacinių sistemų kūrimas, vystymas ir valdymas turi būti vykdomas atsižvelgiant į veiklos ir informacijos saugumo reikalavimus. Sutartyse su paslaugų teikėjais turi būti numatyti visi reikiami saugumo reikalavimai ir įpareigojimai, nustatyti teisės aktuose, reglamentuojančiuose informacinių sistemų kūrimą.

35. ISVS apima šiuos dokumentus:

35.1. Politiką;

35.2. Politiką reglamentuojančius ir su ja susijusius informacijos saugumo srities ŽŪDC teisės aktus;

35.3. pagal ISO 27001 ir ŽŪDC teisės aktus reikalaujamus įrašus.

36. ISVS dokumentai ir įrašai tvarkomi vadovaujantis ŽŪDC nustatyta dokumentų ir įrašų valdymo tvarka.

37. Visa ŽŪDC informacija (įskaitant dokumentus ir įrašus) skirstoma į informacijos klases, atsižvelgiant į reikalavimus jos saugumui.

38. Siekiant užtikrinti greitą, efektyvų ir organizuotą atsaką į informacijos saugos incidentus, informacijos saugos įvykiai ir incidentai registruojami, analizuojami ir sprendžiami, vadovaujantis incidentų valdymą reglamentuojančių informacinių išteklių valdytojų ir ŽŪDC teisės aktų nustatyta tvarka. Veiklos tęstinumo valdymas turi užtikrinti, kad informacijos saugos incidentų pasekmės turėtų kuo mažesnę įtaką ŽŪDC veiklai.

39. Siekiant užtikrinti ISVS ir informacijos saugumo efektyvumą, atliekamas ISVS veiksmingumo matavimas, vadovaujantis ŽŪDC teisės aktais.

40. ISVS vidaus auditas atliekamas periodiškai, ne rečiau kaip kartą per metus patikrinant ir įvertinant ISVS atitiktį ISO 27001 reikalavimams.

41. Vadybos vertinamoji analizė yra skirta ISVS tinkamumui, adekvatumui ir efektyvumui įvertinti. Vadybos ISVS vertinamosios analizės posėdžio metu taip pat priimami sprendimai dėl ISVS tobulinimo galimybių ir ISVS pakeitimų. Vadybos ISVS vertinamąją analizę ne rečiau kaip kartą per metus inicijuoja ISPV.

42. Neatitiktys ir korekciniai veiksmai valdomi ŽŪDC teisės aktuose nustatyta tvarka.

43. ISVS tinkamumas, adekvatumas ir efektyvumas yra nuolat tobulinami, atliekant rizikos vertinimą, veiksmingumo matavimą, vidaus auditą, vadybos ISVS vertinamąją analizę, numatant ir įgyvendinant korekcinius veiksmus.

VI SKYRIUS
BAIGIAMOSIOS NUOSTATOS

44. Politikos reikalavimų turi laikytis visi darbuotojai. Už Politikos reikalavimų laikymąsi kiekvienas darbuotojas atsako asmeniškai.

45. Už informacijos saugumo pažeidimus darbuotojai atsako Lietuvos Respublikos įstatymų ir ŽŪDC teisės aktų nustatyta tvarka.

46. Su informacijos saugumu susiję ŽŪDC teisės aktai rengiami vadovaujantis Politikoje išdėstytomis nuostatomis.

47. Politika turi būti peržiūrima įvykus pokyčiams, galintiems turėti įtakos informacijos saugumui, bet ne rečiau kaip kartą per metus. Už Politikos peržiūrą atsako ISPV.

48. Su Politika ir jos pakeitimais supažindinami visi darbuotojai per dokumentų valdymo sistemą arba kitomis priemonėmis. Kiti naudotojai yra supažindinami su Politika, ją skelbiant ŽŪDC interneto svetainėje www.zudc.lt, ir pagal poreikį kitais ISVS dokumentais.

49. Politika įsigalioja nuo jos patvirtinimo ŽŪDC generalinio direktoriaus įsakymu dienos.

50. Politiką, jos pakeitimus, papildymus, pripažinimą netekusia galios įsakymu tvirtina ŽŪDC generalinis direktorius.

_____