KLAIPĖDOS VANDUO

PATVIRTINTA
Akcinės bendrovės
„KLAIPĖDOS VANDUO“
Generalinio direktoriaus
2022-08-30
įsakymu Nr. 2022/V-ADM.4-4.E-105

AKCINĖS BENDROVĖS „KLAIPĖDOS VANDUO“ MINIMALŪS KIBERNETINIO SAUGUMO REIKALAVIMAI IŠORĖS ŠALIMS

VERSIJA 1

Norminis vidaus teisės aktas	Rengėjas / Savininkas	Patvirtinimo data, Nr.	Statusas	Versija
Akcinės bendrovės „KLAIPĖDOS VANDUO“ minimalūs saugumo reikalavimai taikomi išorės šalims	IT skyrius	2022-08-30 Nr.2022/V-ADM.4-4.E-105	Aktuali redakcija	V.1.

TURINYS

Norminis vidaus teisės aktas	Rengėjas / Savininkas	Patvirtinimo data, Nr.	Statusas	Versija
Akcinės bendrovės „KLAIPĖDOS VANDUO“ minimalūs saugumo reikalavimai taikomi išorės šalims	IT skyrius	2022-08-30 Nr.2022/V-ADM.4-4.E-105	Aktuali redakcija	V.1.

I. BENDROSIOS NUOSTATOS

1.1. Akcinės bendrovės „KLAIPĖDOS VANDUO“ minimalūs saugumo reikalavimai išorės šalims (toliau – Reikalavimai) tikslas – nustatyti akcinės bendrovės „KLAIPĖDOS VANDUO“ (toliau – Bendrovė) informacijos ir kibernetinio saugumo reikalavimus taikomus visiems fiziniams ir juridiniams asmenims, su kuriais Bendrovė sudaro sutartis (raštu, žodžiu) ir tokių sutarčių vykdymas apima Bendrovės valdomos informacijos ir informacinių išteklių apsaugos principus bei jų tvarkymo veiksmus.

1.2. Dokumentas skelbiamas https://www.vanduo.lt .

II. SĄVOKOS IR SUTRUMPINIMAI

2.1. Plane vartojamos šios sąvokos ir trumpiniai:

Išorės šalis	Asmuo, neturintis darbo santykių su Bendrove, bet turintis sutartinius santykius su Bendrove.
Kibernetinis incidentas	Įvykis ar veika, kuri sukelia ar gali sukelti neteisėtą prisijungimą ar sudaryti sąlygas neteisėtai prisijungti prie informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos, sutrikdyti ar pakeisti, įskaitant valdymo perėmimą, informacinės sistemos, elektroninių ryšių tinklo ar pramoninių procesų valdymo sistemos veikimą, sunaikinti, sugadinti, ištrinti ar pakeisti elektroninę informaciją, panaikinti ar apriboti galimybę naudotis elektronine informacija, taip pat sudaryti sąlygas pasisavinti ar kitaip panaudoti neviešą elektroninę informaciją tokios teisės neturintiems asmenim

III. ATITIKTIES REIKALAVIMAI

3.1. Šie Reikalavimai apibrėžia minimalius informacijos ir kibernetinio saugumo principus, kurie turi būti įvykdyti bet kokiomis sąlygomis pagal atitinkamą Sutartį su Bendrove, kurioje yra nuoroda į šiuos Reikalavimus.

3.2. Bendrovės prašymu leisti Bendrovės asmeniui paskirtam už Kibernetinio saugumo užtikrinimą ar kitam Bendrovės įgaliotam asmeniui atlikti informacijos ir kibernetinio saugumo auditą, ar kitus informacijos ir kibernetinio saugumo patikrinimo veiksmus. Taip pat pateikti visą informaciją, kuri reikalinga patikrinti ar Išorės šalis laikosi šių Reikalavimų ir taikomų aktualių informacijos ir kibernetinio saugumo teisės aktų nurodymų.

3.3. Galimi nukrypimai nuo Reikalavimų turi būti dokumentuoti raštu.

3.4. Priklausomai nuo prieigos ir darbo su informacinėmis sistemomis, informacija bei duomenų tinklais gali būti taikomi papildomi techniniai ir organizaciniai reikalavimai nurodyti:

3.4.1. Lietuvos Respublikos vyriausybės 2018 m. gruodžio mėn. 5 d. nutarimu Nr. 1209 „Dėl Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimo Nr. 818 „Dėl

nacionalinės kibernetinio saugumo strategijos patvirtinimo“ pakeitimo“ patvirtintame Organizacinių ir techninių kibernetinio saugumo reikalavimų, taikomų kibernetinio saugumo subjektams, apraše.

3.4.2. 2002 m. spalio mėn. 10 d. Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatyme Nr. IX-1132 (su vėlesniais pakeitimais).

3.4.3. 2020 m. birželio mėn. 18 d. Valstybinės duomenų apsaugos inspekcijos Tvarkomų asmens duomenų saugumo priemonių ir rizikos įvertinimo gairėse duomenų valdytojams ir duomenų tvarkytojams.

IV. NUOTOLINIAI DARBO SAUGUMO REIKALAVIMAI

4.1. Nuotolinė Prieigą Išorės šaliai suteikiama pagal galiojančią bendrovėje Prieigų valdymo tvarką.

4.2. Nuotolinė Prieiga Išorės šaliai suteikiama tik įvertinus potencialias rizikas.

4.3. Išorės šaliai suteikiant galimybę dirbti nuotolinėje kompiuterizuotoje darbo vietoje, priklausančioje Išorės šaliai, bei suteikiant nuotolinę prieigą prie Bendrovės informacinių sistemų (išteklių) būtina:

4.3.1. Naudoti tik saugų VPN ryšį;

4.3.2. Įsitikinti, kad informacinės sistemos, kompiuterinė įranga ir duomenų tinklai iš kurių jungiamasi per nuotolį yra saugūs ir patikimi (atnaujinta operacinė sistema ir kita programinė įranga, įdiegta antivirusinė programinė įranga, įjungta ir sukonfigūruota ugniasienė ir t.t.);

4.3.3. Užtikrinti reguliarią prieigos teisių kontrolę;

4.3.4. Vykdyti nuolatinį veiksmų stebėjimą ir kontrolę;

4.3.5. Užtikrinti bendrovės konfidencialios informacijos, įskaitant asmens duomenų apsaugą tinkamomis techninėmis priemonėmis (pvz. šifruojant informacijos perdavimą, saugojimą ir pan.);

4.3.6. Užtikrinti, kad nuotolinio prisijungimo ryšys būtų kontroliuojamas su iš anksto tarpusavyje suderintais tikslais;

4.3.7. Nuotolinio ryšio sujungimas ir nuotolinės prieigos suteikimas vyktų vadovaujantis principu „Būtina darbui“, bei turėtų sutartą galiojimo terminą.

V. BENDRIEJI KIBERNETINIO SAUGUMO REIKALAVIMAI

5.1. Išorės šalis turi užtikrinti, kad bet kokia nauja jos įdiegta technologija Bendrovėje yra sankcionuota ir yra gautas bendrovės įgaliotų asmenų sutikimas ją naudoti, taip pat užtikrinti, kad šios technologijos informacijos ir kibernetinė sauga yra pakankama.

5.2. Informacinių sistemų naudotojas ar administratorius turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone ir papildomu autentifikavimo faktoriumi (jei informacinė sistema palaiko tokį funkcionalumą).

5.3. Suteikiant laikinus slaptažodžius Informacinių sistemų naudotojams ir administratoriams, šie slaptažodžiai turi būti unikalūs kiekvienam ištekliaus naudotojui ir perduodami saugiu būdu.

5.4. Slaptažodžiai negali būti saugomi ar perduodami atviru tekstu. Tik laikinas slaptažodis gali būti perduodamas atviru tekstu, tačiau atskirai nuo naudotojo vardo, jeigu Informacinių sistemų naudotojas neturi galimybių iššifruoti gauto užšifruoto slaptažodžio, ar nėra techninių galimybių Informacinių sistemų naudotojui perduoti slaptažodį šifruotu kanalu, ar saugiu elektroniniu ryšių tinklu.

5.5. Visose Informacinėse sistemose, prieš pradedant jas eksploatuoti, Informacinių sistemų administratoriai privalo pakeisti standartinius (gamintojų) slaptažodžius į šiuos Reikalavimus atitinkančius slaptažodžius.

5.6. Informacinių sistemų dalys, patvirtinančios Informacinių sistemų naudotojo tapatumą, turi drausti automatiškai išsaugoti slaptažodžius.

5.7. Informacinių sistemų administratoriaus funkcijos turi būti atliekamos, naudojant atskirą tam skirtą naudotojo vardą, kuris negali būti naudojamas kasdienėms Informacinių sistemų naudotojo funkcijoms atlikti.

5.8. Informacinių sistemų naudotojams negali būti suteikiamos Informacinių sistemų administratoriaus teisės.

5.9. Kiekvienas Informacinių sistemų naudotojas ar administratorius turi būti unikaliai atpažįstamas.

5.10. Informacinėse sistemose turi būti išjungiamos visos nereikalingos gamyklinės naudotojų paskyros (tame tarpe svečio paskyra).

5.11. Viešai prieinamose kompiuterizuotose darbo vietose paskutinio naudotojo vardas neturi būti matomas prisijungimo metu.

5.12. Prieiga turi būti suteikiama vadovaujantis principu „Būtina darbui“.

5.13. Prisijungdamas nuotoline prieiga prie Informacinių sistemų, naudotojas turi patvirtinti savo tapatybę slaptažodžiu arba kita tapatumo patvirtinimo priemone.

5.14. Bet kokia nesankcionuota nuotolinė prieiga prie Bendrovės informacinių sistemų ir duomenų ar įrangos turi būti draudžiama.

5.15. Nuotolinė prieiga prie Bendrovės informacinių sistemų ir duomenų tinklo iš viešųjų duomenų tinklų turi būti šifruojama taikant VPN technologiją.

VI. PAPILDOMI KIBERNETINIO SAUGUMO REIKALAVIMAI TECHNOLOGINĖMMS PROCESŲ VALDYMO SISTEMOMS

6.1. Gamybinių procesų valdymo sistemos ir jų duomenų tinklas, bei jo komponentai negali turėti nuotolinės prieigos iš viešųjų duomenų tinklų.

6.2. Gamybiniame duomenų tinkle informacinių išteklių (tarnybinių stočių, komutatorių, maršrutizatorių, ugniasienių ir pan.) administravimui turi būti naudojama atskira techninė įranga neturinti el. pašto paskyros, prieigos prie viešųjų duomenų tinklų ar naudojama darbui su konfidencialia informacija.

VII. DIEGIAMOS AR KŪRIAMOS SAUGIOS PROGRAMINĖS ĮRANGOS REIKALVIMAI

7.1. Išorės šalis nustato, dokumentuoja ir įgyvendina iniciatyvas, atitinkančias bendrai priimtus informacijos ir kibernetinio saugumo standartus bei praktiką siekiant sukurti saugius programinės ar techninės įrangos kūrimo procesus. Tokios iniciatyvos turi užtikrinti informacijos ir kibernetinį saugumą visuose plėtros etapuose: mokymuose, reikalavimų apibrėžimuose, dizaino kūrime, diegime, patvirtinime, išleidime ir priežiūroje.

7.2. Programinė įranga neturi naudotojo paskyrų, slaptažodžių ar privačių/slaptų raktų, kurių negali pakeisti arba pašalinti įgaliotasis produkto galutinis vartotojas.

7.3. Programinė įranga neturi jokių naudotojo paskyrų (individualių, bendrų, testavimo aplinkos), kurios nėra dokumentuotos (tai nereiškia, kad susijusių naudotojų prieigos duomenys turi būti atskleisti).

7.4. Išorės šalis turi aktyviai imtis priemonių, kad būtų pagerinta produkto saugumo kokybė. Šios priemonės turi atitikti bendrai priimtus IT ir technologinių procesų valdymo kibernetinio saugumo standartus ir praktiką bei, jei tai techniškai įmanoma, apimti patikimumo bandymus, pažeidžiamumų valdymą ir programinio kodo saugumo testavimus (įskaitant statinio ar binarinio kodo analizę).

7.5. Turi būti užtikrinta kuriamo programinio kodo higiena (negali būti pavyzdinės imties duomenų ir scenarijaus kodo, nuorodų į nenaudojamas bibliotekas, derinimo kodo ir kt. naudotų įrankių) perkeliant vystomą programinę įrangą į darbinę aplinką.

7.6. Vystomos programinės įrangos kūrimo, testavimo ir darbinės aplinkos turi būti atskirtos. Programinės įrangos kūrimas turi būti atliekamas specialioje aplinkoje, kuri nėra prijungta prie IT sistemų, naudojamų tvarkant asmens duomenis. Testuojant sistemas, turi būti naudojami testiniai duomenys. Tais atvejais, kai tai neįmanoma, turi būti nustatytos specialios testavimo metu naudojamų asmens duomenų apsaugos procedūros.

7.7. Programinės įrangos galutiniams naudotojams neturi būti rodomi vystomos programinės įrangos klaidų apie programinį kodą ar tarnybinės stoties pranešimai.

7.8. Diegiama ar kuriama programinė įrangą turi atsižvelgti į rekomendacijas pateikiamas https://www.nksc.lt/rekomendacijos.html

7.9. Įdiegta programinė įranga Bendrovės įgaliotų asmenų nuskanuojama su pažeidžiamumų skanavimo įrankiu. Rasti pažeidžiamumai, įvertinus rizikas, turi būti išorės šalių užkardomi.

VIII. FIZINĖS SAUGOS REIKALAVIMAI

8.1. Išorės šalių atstovai ir jų transporto priemonės į bendrovės objektų teritorijas įleidžiami tik su Bendrovės išduotais leidimais arba su lydinčio Bendrovės darbuotojo žinia.

8.2. Visi Bendrovės išduoti leidimai yra vardiniai, juos draudžiama perduoti ir/ar kitokiu būdu perleisti naudotis tretiesiems asmenims.

8.3. Bendrovės teritorijose draudžiama filmuoti ar fotografuoti negavus už Bendrovės atsakingų asmenų leidimo.

8.4. Draudžiama į bendroves teritoriją įvežti/įnešti šiuos daiktus:

8.4.1. Lietuvos Respublikos Ginklų ir šaudmenų kontrolės įstatyme įrašytus visų kategorijų ginklus, jų priedėlius ir šaudmenis ar jų imitacijas;

8.4.2. Sprogstamuosius įtaisus, sprogiąsias medžiagas ar jų imitacijas;

8.4.3. Narkotikus, narkotines medžiagas bei alkoholinius gėrimus;

8.4.4. Kitus atvirą liepsną naudojančius ar kibirkštį skleidžiančius/sukeliančius, pavojingus daiktus, išskyrus tiesioginiam darbui, kuriam turi būti išduotas leidimas, naudojamus įrankius ar prietaisus.

IX. IŠORĖS ŠALIES ĮSIPAREIGOJIMAI

9.1. Išorės šalis įsipareigoja:

9.1.1. Laikytis šių Reikalavimų.

9.1.2. Bendrovėje įdiegtų saugumą bei asmens duomenų apsaugą užtikrinančių procesų.

9.1.3. Be išankstinio raštiško sutikimo neatskleisti tvarkomų asmens duomenų, konfidencialios Bendrovės informacijos jokioms trečiosioms šalims ar gavėjams.

9.1.4. Dirbdama su Bendrovės informaciniais ištekliais vadovautis ir laikytis Informacijos ir kibernetinio saugumo politikos, šių Reikalavimų, kitų įdiegtų Bendrovės informacijos ir kibernetinio saugumo procesų bei nustatytų prievolių, su kuriomis supažindina už Išorės šalį atsakingas Bendrovės darbuotojas.

9.1.5. Atsakyti už visus duomenų perdavimo tinklams ar informacinėms sistemoms Išorės šalies raštišku prašymu suteiktų informacinių sistemų naudotojų ar jų prašyme nurodytų asmenų kaltės atliktus žalingus veiksmus ir jais Bendrovei padarytus nuostolius.

9.1.6. Užtikrinti Bendrovės informacinės sistemos elektroninės informacijos konfidencialumą bei vientisumą, savo veiksmais netrikdyti informacinės sistemos prieinamumo.

9.1.7. Saugoti tvarkomus asmens duomenis.

9.1.8. Naudoti tik tas prieigos prie informacinės sistemos teises (sukurti, redaguoti, papildyti ar panaikinti), kurios buvo suteiktos.

9.1.9. Naudotis tik tomis informacinės sistemos funkcijomis ir tokia informacijos apimtimi informacinėse sistemose, prie kurios prieiga jam suteikta vadovaujantis prieigų suteikimą prie informacinių išteklių reglamentuojančiais dokumentais.

9.1.10. Nedelsiant, tačiau ne vėliau nei per 24 val. po to, kai sužinojo apie tai, raštu informuoti Bendrovę apie Informacijos ir kibernetinio saugumo incidentą, kuris gali būti susijęs su asmens duomenimis, informaciniais ištekliais ar duomenų perdavimo tinklu, pateikiant visą turimą informaciją bei duomenis, susijusius su tokiu pažeidimu.

9.1.11. Užtikrinti, kad imsis pakankamų priemonių rizikoms susijusioms su subrangovais, jų atliekamais darbais ir tiekimo grandine suvaldyti.

9.1.12. Tais atvejais kai bus tvarkomi asmens duomenys, sudaryti nustatytos formos duomenų tvarkymo susitarimą.

9.1.13. Pateikti informaciją apie taikomas duomenų saugumo priemones, užpildant apklausos anketą dėl taikomų asmens duomenų apsaugos priemonių duomenų tvarkytojams bei kitus prašomus dokumentus taikomoms duomenų saugumo priemonėms pagrįsti.

9.2. Išorės šaliai draudžiama:

9.2.1. Skenuoti Bendrovės informacines sistemas ar bendrovės duomenų perdavimo tinklą, ieškant pažeidžiamumų ar kitais būdais stebėti duomenų perdavimo tinklo srautą. Jei šiame punkte išvardintos priemonės, reikalingos tiesioginėms pareigoms atlikti, jas panaudoti galima tik suderinus su už informacijos ir kibernetinį saugumą atsakingu asmeniu.

9.2.2. Be atskiro Bendrovės atsakingo asmens leidimo ir žinios prie bendrovės duomenų perdavimo tinklo ar informacinių sistemų jungtis naudojant ne Bendrovės išduotą įrangą (išskyrus svečiams skirtame belaidžiame tinkle).

9.2.3. Gerti, valgyti ir rūkyti šalia informacijos apdorojimo priemonių, bendrovės serverinėse ar prie bendrovės komutacinių spintų.

9.2.4. Savavališkai keisti suteiktus tinklo parametrus (IP adresą ir pan.) ir kitą konfigūraciją.

9.2.5. Naudoti programas, kurios gali trikdyti Bendrovės informacinių sistemų bei duomenų perdavimo tinklo veikimą (duomenų perdavimo tinklo skenavimo ir blokavimo programos ir pan.).

9.2.6. Savarankiškai keisti ir taisyti Bendrovės išduotą techninę ir programinę įrangą.

9.2.7. Naudoti bendrovės išduotą techninę ir programinę įrangą Lietuvos Respublikos įstatymais draudžiamai veiklai, šmeižikiško, įžeidžiančio, grasinamojo pobūdžio ar visuomenės dorovės ir moralės principams prieštaraujančiai veiklai, kompiuterių virusams, masinei piktybiškai informacijai siųsti ar kitiems tikslams, kurie gali pažeisti Bendrovės ar kitų asmenų teisėtus interesus.

9.2.8. Diegti, saugoti naudoti, kopijuoti ar platinti nelegalią, autorines teises pažeidžiančią programinę įrangą.

9.2.9. Diegti įrangą bendrovės infrastruktūroje nesuderinus su įgaliotų įmonės darbuotoju.

9.3. Išorės šalis turi vykdyti savo darbuotojų informacijos ir kibernetinio saugumo sąmoningumo ugdymą suteikiant technines, procedūrines ir saugios veiklos kibernetinėje erdvėje žinias.

9.4. Išorės šalies darbuotojai ir jai dirbantys asmenys privalo pateikti atitinkantį kvalifikacijos įrodymą leidžiantį dirbti su konkrečiu Bendrovės informaciniu ištekliu kur tai yra būtina arba reikalaujama.

9.5. Išorės šalis turi būti pasitvirtinusi informacijos ir kibernetinių incidentų valdymo bei veiklos tęstinumo planus ar kitą dokumentaciją, reglamentuojančią Išorės šalies darbuotojų veiksmus informacijos ir kibernetinių incidentų metu.

X. ATSAKOMYBĖ IR GINČŲ SPRENDIMO TVARKA

10.1. Kiekvienas ginčas, nesutarimas ar reikalavimas, kylantis iš Reikalavimų ar susijęs su Reikalavimais, jų pažeidimu, nutraukimu bei galiojimu, turi būti sprendžiamas Sutartyje nustatyta tvarka.

10.2. Išorės šalis yra atsakinga už visas būtinas priemones ir veiksmus siekiant laikytis šių Reikalavimų bei kituose taikomuose teisės aktuose nustatytų pareigų vykdymą.

10.3. Jei dėl Išorės šalies veiksmų ar neveikimo vykdant Sutartį Lietuvos Respublikos kibernetinio saugumo įstatyme numatytoms kontroliuojančioms institucijoms nustačius informacijos ir kibernetinio saugumo pažeidimą Bendrovės skiriama piniginė sankcija, Išorės šalis įsipareigoja Bendrovei pareikalavus atlyginti Bendrovei tokios sankcijos sumą, laikantis Sutartyje numatytos baudų sumokėjimo Bendrovei tvarkos.

10.4. Už Išorės šalies pasitelktų Subrangovų vykdomą tinkamą Reikalavimų įgyvendinimą prieš Bendrovę atsako Išorės šalis.

XI. BAIGIAMOSIOS NUOSTATOS

11.1. Reikalavimų galiojimas Išorės šaliai yra neatsiejamas nuo Bendrovės ir Išorės šalies sudarytos Sutarties galiojimo termino.

11.2. Bet kurios iš Reikalavimų sąlygos pripažinimo negaliojančia dėl prieštaravimo imperatyvioms teisės aktų nuostatoms atveju, ši sąlyga keičiama, vadovaujantis bendra Sutartyje nustatyta tvarka.

11.3. Šie Reikalavimai nėra atskirai pasirašomi. Reikalavimai yra skelbiami Bendrovės internetiniame puslapyje https://www.vanduo.lt arba kitame Išorės šaliai prieinamame šaltinyje, arba sudarant kitokią individualią ar viešo pobūdžio prieigą prie Reikalavimų.