Kibernetinio saugumo, susijusio su trečių šalių teikiamomis paslaugomis ar parduodamomis prekėmis, valdymo tvarkos aprašo 5 priedas

(Klausimyno forma)

ATTIKTIES KIBERNETINIO SAUGUMO IR ASMENS DUOMENŲ APSAUGOS REIKALAVIMAMS KLAUSIMYNAS

Duomenų valdytojas: UAB „Vilniaus vandenys“

Duomenų tvarkytojas: (Įrašyti)

Klausimai		Atsakymai	Valdytojo komentarai	Tvarkytojo komentarai
Bendri klausimai				
1.	Ar esate kibernetinio saugumo subjektas pagal Lietuvos Respublikos kibernetinio saugumo įstatymą (toliau – KSĮ)?	☐ Taip ☐ Ne	Nurodykite: 1. esate esminis ar svarbus subjektas; 2. ar esate įgyvendinę visus KSĮ nustatytus reikalavimus, jei ne – iki kada planuojate juos įgyvendinti.	
2.	Ar turite dedikuotą ir nuo IT administravimo atskirą funkciją, atsakingą už žurnalinių įrašų nuolatinį stebėjimą ir incidentų valdymą (lygiavertę KSĮ lydinčiuosiuose teisės aktuose nurodomai Saugumo operacijų centro (SOC) funkcijai)?	☐ Taip ☐ Ne	Nurodykite: 1. ar SOC (ar lygiavertę) vykdote patys, ar pasitelkiate išorės tiekėją; 2. jei pasitelkiamas išorės tiekėjas, prašome jį nurodyti.	
3.	Ar esate sertifikavę savo kibernetinio saugumo ar informacijos saugos procesus, susijusius su UAB „Vilniaus vandenys“ teikiamomis ar planuojamomis teikti paslaugoms, tarptautiniu mastu pripažįstamu standartu (pvz. ISO 27001 arba lygiaverčiu)?	☐ Taip ☐ Ne	Pateikite sertifikato kopiją.	
Žmogiškieji ištekliai				
4.	Ar esate paskyrę už kibernetinį saugumą atsakingą vadovybės atstovą (KSĮ nurodytą kibernetinio saugumo vadovą ar lygiavertę pareigybę)?	☐ Taip ☐ Ne	Nurodykite: 1. asmenį, atliekantį kibernetinio saugumo vadovo (ar lygiavertes) funkcijas; 2. jo kompetencijas saugumo srityje (išsilavinimas, sertifikatai, patirtis ir pan.).	

5.	Ar Jūsų darbuotojai yra pasirašę įsipareigojimus dėl konfidencialumo dirbant su asmens duomenimis arba konfidencialumo nuostatos yra įtrauktos į darbuotojų darbo sutartis?	☐ Taip ☐ Ne	Pateikite pavyzdį.	
6.	Ar Jūsų įmonėje yra paskirtas už duomenų tvarkymo sutartyje numatytų kibernetinio saugumo priemonių įgyvendinimą atsakingas asmuo, turintis tinkamos kompetencijos kibernetinio saugumo srityje?	☐ Taip ☐ Ne	Nurodykite: 1. asmenį, atsakingą už saugumo priemonių įgyvendinimą; 2. atsakingo asmens kompetencijas saugumo srityje (išsilavinimas, sertifikatai, patirtis ir pan.).	
7.	Ar Jūsų įmonėje vykdomi periodiniai kibernetinio saugumo / duomenų apsaugos mokymai, instruktažai darbuotojams?	☐ Taip ☐ Ne	Pateikite informaciją, kada paskutinį kartą buvo vykdomi kibernetinio saugumo / duomenų apsaugos mokymai darbuotojams.	
Asmens duomenų apsaugos politika ir kitos procedūros				
8.	Ar Jūsų įmonėje yra patvirtinta asmens duomenų apsaugos politika? Jeigu asmens duomenų apsaugos politika yra informacijos saugumo (kibernetinio saugumo) politikos dalis – žymėkite atsakymą taip.	☐ Taip ☐ Ne	Nurodykite dokumento patvirtinimo datą ir numerį. Pateikite informaciją, kokiu periodiškumu atnaujinama / keičiama duomenų apsaugos politika.	
9.	Ar įmonėje yra patvirtintas duomenų saugumo pažeidimų valdymo procesas (tvarka), kuriame būtų reglamentuota, kaip teikiamas pranešimas duomenų valdytojui apie duomenų saugumo pažeidimus, susijusius su tvarkomais duomenų valdytojo duomenimis?	☐ Taip ☐ Ne	Nurodykite dokumento patvirtinimo datą ir numerį.	
10.	Ar turite duomenų saugumo pažeidimų registrą?	☐ Taip ☐ Ne		
11.	Ar per paskutinius metus savo praktikoje turėjote duomenų saugumo pažeidimų?	☐ Taip ☐ Ne	Nurodykite, kiek saugumo pažeidimų įvyko per paskutinius metus ir kokie pagrindiniai veiksniai, dėl kurių įvyko duomenų saugumo pažeidimai.	

12.	Ar pildote duomenų veiklos įrašus?	☐ Taip ☐ Ne	Pateikite informaciją, kokiu periodiškumu atnaujinami / peržiūrimi veiklos įrašai?	
Kompiuterinė ir programinė įranga. Prieigos kontrolės valdymas. Veiklos tęstinumo valdymas				
13.	Ar kompiuterizuotose darbo vietose (toliau – KDV) ir serveriuose naudojama gamintojų palaikoma informacijos apdorojimo sistemos fizinių komponentų visuma arba tos visumos dalis?	☐ Taip ☐ Ne		
14.	Ar KDV ir serveriuose naudojama informacinės technologijos ir telekomunikacijos (toliau – ITT) paslaugų teikėjo įdiegta ir prižiūrima operacinė sistema?	☐ Taip ☐ Ne	Nurodykite, kokios operacinės sistemos naudojamos KDV ir serveriuose.	
15.	Ar įdiegtos kritinius ir svarbius programinės įrangos (toliau – PĮ) saugumo pažeidžiamumus taisančios pataisos?	☐ Taip ☐ Ne	Kada paskutinį kartą tokios pataisos ir kokiai PĮ buvo diegtos?	
16.	Ar naudotojams yra taikomi apribojimai diegti, šalinti, administruoti neautorizuotą programinę įrangą?	☐ Taip ☐ Ne		
17.	Ar darbui ir KDV administravimui naudojamos atskiros paskyros?	☐ Taip ☐ Ne	Patvirtinkite ir pateikite prieigų valdymo atvaizdą (pvz. ekrano nuotrauką).	
18.	Ar IT sistemos turi nustatytą sesijos laiką, t.y. ar naudotojui esant vartotojui neaktyviam sistemoje nustatytą laiką, jo sesija nutraukiama?	☐ Taip ☐ Ne	Nurodykite, koks neaktyvios sesijos laikas taikomas.	
19.	Ar turite patvirtintas slaptažodžių naudojimo taisykles?	☐ Taip ☐ Ne	Pateikite informaciją, kokie reikalavimai taikomi slaptažodžiui: minimalus slaptažodžio ilgis, sudėtingumas, galiojimo laikas, nesėkmingų bandymų įvesti slaptažodį skaičius.	
20.	Ar jungiantis prie valdytojo sistemų taikomas kelių veiksnių autentifikavimas?	☐ Taip ☐ Ne		

21.	Ar apribota kitų Jūsų darbuotojų prieiga prie valdytojo turto (principas „būtina žinoti“)?	☐ Taip ☐ Ne		
22.	Ar naudojama realiu laiku veikianti antivirusinė PĮ (privalo pasileisti ir būti aktyvi sistemos pasileidimo metu)?	☐ Taip ☐ Ne	Nurodykite: 1. kokia (-ios) antivirusinė PĮ naudojama; 2. kada paskutinį kartą atnaujinta (pridėkite ekrano nuotrauką); 3. kokiu periodiškumu atnaujinama antivirusinė (-ės) programa (-os)?	
23.	Ar duomenų judėjimas iš, į IT sistemą stebimas ir kontroliuojamas naudojant ugniasienes ir įsibrovimo (įsilaužimo) aptikimo ir prevencijos sistemas (IDS/IPS)?	☐ Taip ☐ Ne	Nurodykite: 1. kokia ugniasienė naudojama; 2. pateikite ugniasienės dalies taisyklių ekrano nuotrauką.	
24.	Ar naudojate šifruotą komunikacijos kanalą, t.y. kriptografinius protokolus (pvz., TLS/SSL), kai prieiga prie naudojamų IT sistemų vykdoma internetu?	☐ Taip ☐ Ne	Nurodykite, kokia šifravimo PĮ naudojama ir pateikite nustatymų ekrano nuotrauką.	
25.	Ar visoms sistemoms, kuriose Valdytojo pavedimu tvarkomi duomenys yra įgyvendinti techninių žurnalų įrašai?	☐ Taip ☐ Ne	1. Pateikite sistemos žurnalo įrašo kopiją ar ekrano nuotrauką (printscreen, JPG formatu);	
26.	Ar turite įdiegtą apsaugą nuo kenkėjiškų programų, tam kad bet kokia programinė įranga, kuri naudojama teikiant paslaugas Valdytojui, būtų apsaugota nuo kenkėjiškų programų?	☐ Taip ☐ Ne	Nurodykite, kokia apsauga naudojama nuo kenkėjiškos programinės įrangos.	
27.	Ar turite atsarginių kopijų ir duomenų atstatymo procedūras?	☐ Taip ☐ Ne	Pridėkite atsarginių kopijų valdymo sistemos ekrano nuotrauką; Pateikite informaciją, kokiu dažnumu daroma atsarginė pridedamoji, pilna atsarginė kopijos.	
28.	Ar turite mobiliųjų, nešiojamųjų įrenginių naudojimo procedūras?	☐ Taip ☐ Ne	Nurodykite dokumento patvirtinimo datą ir numerį.	
29.	Ar turite IT išteklių registrą?	☐ Taip ☐ Ne	Pateikite informaciją, kokiu periodiškumu peržiūrimas ir atnaujinamas šis registras.	

30.	Ar kasmet vykdomas prasiskverbimo testavimas (angl. P*enetration* testing)?	☐ Taip ☐ Ne	Pateikite informaciją, kada atliktas paskutinis nepriklausomas pažeidžiamumų skenavimas.	
31.	Ar Jūsų įmonėje nustatyta ir įgyvendinta veiklos tęstinumo valdymo ir veiklos atsparumo politika ir procedūros. Ar išbandomas veiklos tęstinumo valdymo planas bent kartą per metus?	☐ Taip ☐ Ne	Nurodykite dokumento patvirtinimo datą ir numerį. Pateikite informaciją, kada atliktas paskutinis veiklos tęstinumo valdymo planas.	
	Debesijos paslaugos			
32.	Ar pasitelkiate debesijos paslaugas iš valdytojo gautų asmens duomenų tvarkymui?	☐ Taip ☐ Ne	Nurodykite debesijos paslaugas jums teikiančius paslaugos tiekėjus.	
33.	Patvirtinkite, kad paslaugų duomenų centrai yra Europos ekonominės erdvės šalyje.	☐ Taip ☐ Ne		
34.	Patvirtinkite, kad debesijos paslaugas teikiantis paslaugos tiekėjas yra sertifikuotas pagal ISO 27001 standartą.	☐ Taip ☐ Ne	Pateikite sertifikato kopiją.	

Įgaliotas Tvarkytojo atstovas:

_____

(pareigos, vardas, pavardė, parašas, data)