

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
<i>Bendri klausimai</i>			
1. Ar esate kibernetinio saugumo subjektas pagal Lietuvos Respublikos kibernetinio saugumo įstatymą (toliau – KSĮ)?	<input type="checkbox"/> Taip <input type="checkbox"/> 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)?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite: 1. ar SOC (ar lygiavertę) vykdate 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 lygiavertę)?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Pateikite sertifikato kopiją.	
<i>Žmogiškieji ištekliai</i>			
4. Ar esate paskyrę už kibernetinį saugumą atsakingą vadovybės atstovą (KSĮ nurodytą kibernetinio saugumo vadovą ar lygiavertę pareigybę)?	<input type="checkbox"/> Taip <input type="checkbox"/> 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?	<input type="checkbox"/> Taip <input type="checkbox"/> 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?	<input type="checkbox"/> Taip <input type="checkbox"/> 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?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Pateikite informaciją, kada paskutinį kartą buvo vykdomi kibernetinio saugumo / duomenų apsaugos mokymai darbuotojams.	
<i>Asmens duomenų apsaugos politika ir kitos procedūros</i>				
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.	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite dokumento patvirtinimo datą ir numerį. Pateikite informaciją, koku 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?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite dokumento patvirtinimo datą ir numerį.	
10.	Ar turite duomenų saugumo pažeidimų registrą?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne		
11.	Ar per paskutinius metus savo praktikoje turėjote duomenų saugumo pažeidimų?	<input type="checkbox"/> Taip <input type="checkbox"/> 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?	<input type="checkbox"/> Taip	Pateikite informaciją, koku periodiškumu atnaujinami / peržiūrimi veiklos įrašai?	

Ne*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?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne		
14.	Ar KDV ir serveriuose naudojama informacinės technologijos ir telekomunikacijos (toliau – ITT) paslaugų teikėjo įdiegta ir prižiūrima operacinė sistema?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite, kokios operacinės sistemos naudojamos KDV ir serveriuose.	
15.	Ar įdiegtos kritinius ir svarbius programinės įrangos (toliau – PJ) saugumo pažeidžiamumus taisančios pataisos?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Kada paskutinį kartą tokios pataisos ir kokiai PJ buvo diegtos?	
16.	Ar naudotojams yra taikomi apribojimai diegti, šalinti, administruoti neautorizuotą programinę įrangą?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne		
17.	Ar darbui ir KDV administravimui naudojamos atskiros paskyros?	<input type="checkbox"/> Taip <input type="checkbox"/> 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?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite, koks neaktyvios sesijos laikas taikomas.	
19.	Ar turite patvirtintas slaptažodžių naudojimo taisykles?	<input type="checkbox"/> Taip <input type="checkbox"/> 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 veiksmų autentifikavimas?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne		
21.	Ar apribota kitų Jūsų darbuotojų prieiga prie valdytojo turto (principas „būtina žinoti“)?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne		

22.	Ar naudojama realiu laiku veikianti antivirusinė PĮ (privalo pasileisti ir būti aktyvi sistemos pasileidimo metu)?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite: 1. kokia (-ios) antivirusinė PĮ naudojama; 2. kada paskutinį kartą atnaujinta (pridėkite ekrano nuotrauką); 3. koku 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)?	<input type="checkbox"/> Taip <input type="checkbox"/> 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?	<input type="checkbox"/> Taip <input type="checkbox"/> 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?	<input type="checkbox"/> Taip <input type="checkbox"/> 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?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite, kokia apsauga naudojama nuo kenkėjiškos programinės įrangos.	
27.	Ar turite atsarginių kopijų ir duomenų atstatymo procedūras?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Pridėkite atsarginių kopijų valdymo sistemos ekrano nuotrauką; Pateikite informaciją, koku dažnumu daroma atsarginė pridedamoji, pilna atsarginė kopijos.	
28.	Ar turite mobiliųjų, nešiojamųjų įrenginių naudojimo procedūras?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite dokumento patvirtinimo datą ir numerį.	
29.	Ar turite IT išteklių registrą?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Pateikite informaciją, koku periodiškumu peržiūrimas ir atnaujinamas šis registras.	
30.	Ar kasmet vykdomas prasiskverbimo testavimas (angl. <i>Penetration testing</i>)?	<input type="checkbox"/> Taip <input type="checkbox"/> 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?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite dokumento patvirtinimo datą ir numerį. Pateikite informaciją, kada atliktas paskutinis veiklos tęstinumo valdymo planas.	
<i>Debesijos paslaugos</i>				
32.	Ar pasitelkiate debesijos paslaugas iš valdytojo gautų asmens duomenų tvarkymui?	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Nurodykite debesijos paslaugas jums teikiančius paslaugos tiekėjus.	
33.	Patvirtinkite, kad paslaugų duomenų centrai yra Europos ekonominės erdvės šalyje.	<input type="checkbox"/> Taip <input type="checkbox"/> Ne		
34.	Patvirtinkite, kad debesijos paslaugas teikiantis paslaugos tiekėjas yra sertifikuotas pagal ISO 27001 standartą.	<input type="checkbox"/> Taip <input type="checkbox"/> Ne	Pateikite sertifikato kopiją.	

Įgaliotas Tvarkytojo atstovas:

(pareigos, vardas, pavardė, parašas, data)