Vilniaus vandenys

PATVIRTINTA
2023-09-28 Nr. VTA-I23-248

GENERALINIS DIREKTORIUS

ĮSAKYMAS
DĖL VALDYBOJE PATVIRTINTOS UAB „VILNIAUS VANDENYS“ INFORMACIJOS SAUGUMO POLITIKOS TAIKYMO IR SUPAŽINDINIMO

Užtikrinant informacijos saugumą Bendrovėje ir vadovaujantis 2023 m. rugsėjo 14 d. Valdybos posėdžio protokolu Nr. PR-V23-12 patvirtinta UAB “Vilniaus vandenys” Informacijos saugumo politika (pridedama) (toliau – Politika):

1. Įpareigoju visiems Bendrovės darbuotojams vadovautis Politikoje įtvirtintais įsipareigojimais, principais ir atsakomybėmis.

2. Nustatau, kad už tinkamą šio įsakymo vykdymą atsakingi visi Bendrovės struktūrinių padalinių vadovai, o už tinkamą šio įsakymo vykdymo kontrolę atsakingas Veiklos atsparumo skyriaus vadovas.

3. Nustatau, kad visi esami ir naujai priimami Bendrovės darbuotojai privalo susipažinti su Politika ir laikytis joje įtvirtintų nuostatų.

4. Įpareigoju padalinių vadovus, per 20 kalendorinių dienų, pasirašytinai supažindinti savo darbuotojus, kurie neturi kompiuterizuotos darbo vietos.

5. Pripažįstu netekusiu galios generalinio direktoriaus 2022 m. balandžio 7 d. įsakymą Nr. VTA-I22-72 ,,Dėl UAB „Vilniaus vandenys“ Kibernetinio ir informacijos saugumo politikos patvirtinimo“.

6. Pavedu Komunikacijos skyriui Informacijos saugumo politiką paskelbti Bendrovės interneto svetainėje.

Generalinis direktorius Saulius Savickas

Rengė: Julius Lisauskas, el. p. julius.lisauskas@vv.lt
Supažindinti: visus Bendrovės darbuotojus.

UAB „Vilniaus vandenys“ informacijos saugumo politika

Tikslas	Informacijos saugumo politika (toliau – Politika) yra skirta nustatyti UAB „Vilniaus vandenys“ informacijos saugumo valdymo principus, efektyvias saugumo užtikrinimo kryptis, siekiant suvaldyti grėsmių sukeliamas informacijos saugos rizikas, užtikrinti TIS2 ir kitų Europos Sąjungos, Lietuvos Respublikos teisės aktų atitiktį.
Taikymo sritis	Visos Bendrovės suinteresuotos šalys.
Susiję teisės aktai	Bendrovės informacinių sistemų duomenų saugos nuostatai; Informacinių sistemų naudotojų administravimo taisyklės; Saugaus elektroninės informacijos tvarkymo taisyklės; Informacinių sistemų veiklos tęstinumo valdymo planas; Bendrovėje atsakingų asmenų už organizacinių ir techninių kibernetinio saugumo reikalavimų įgyvendinimą ir kontrolę sąrašas; Bendrovės naudojamų techninių kibernetinio saugumo priemonių sąrašas; UAB „Vilniaus vandenys“ suinteresuotų šalių santykių valdymo politika ir planas; UAB „Vilniaus vandenys“ asmens duomenų tvarkymo ir saugumo politika ir jos įgyvendinimo taisyklės; UAB „Vilniaus vandenys“ rizikų valdymo politika; UAB „Vilniaus vandenys“ rizikų valdymo tvarkos aprašas; UAB „Vilniaus vandenys“ veiklos strategijos dokumentas.
Nuorodos	Europos parlamento ir tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148 (TIS2 direktyva); Lietuvos Respublikos kibernetinio saugumo įstatymas; Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas; Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas; Standartas ISO/IEC 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga –Informacijos saugumo valdymo sistemos – Reikalavimai“; Standartas ISO/IEC 27002:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga – Informacijos saugumo kontrolės priemonės“.

Turinys

1. SPECIALIOSIOS SĄVOKOS IR SUTRUMPINIMAI

Bendrovė	UAB „Vilniaus vandenys“
Informacija	Visa Bendrovės gaunama, tvarkoma, kuriama, valdoma ir naudojama žodinė, rašytinė ir elektroninė informacija.
Informacijos saugumas	Informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas; taip pat informacijos saugumas apima tokias informacijos savybes kaip informacijos autentiškumas,

	atskaitingumas, neiššižadėjimas ir patikimumas; Informacijos saugumas apima kibernetinį saugumą ir asmens duomenų apsaugą.
Informaciniai ištekliai	Bendrovės veiklos procesai ir informacija, kurią valdo ir tvarko Bendrovė, atlikdama teisės aktuose nustatytas funkcijas, ir informacinių technologijų priemonės, naudojamos informacijai tvarkyti.
ISO 27001	Standartas ISO/IEC 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga – Informacijos saugumo valdymo sistemos – Reikalavimai“.
ISVS	Rizikų valdymu pagrįsta Informacijos saugumo valdymo sistema, kuria siekiama sukurti, įgyvendinti, valdyti, stebėti, vertinti, prižiūrėti ir gerinti Bendrovės informacijos saugumą.
Kibernetinis saugumas	Visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, aptikti, analizuoti ir reaguoti į juos, taip pat įprastinei elektroninių ryšių tinklų, informacinių sistemų ar pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.
Konfidencialumas	Informacijos savybė, reiškianti, kad su informacija gali susipažinti tik įgalioti asmenys.
Politika	UAB „Vilniaus vandenys“ informacijos saugumo politika.
Prieinamumas	Informacijos savybė, reiškianti, kad informacija gali būti tvarkoma reikiamu metu.
Rizikų valdymo priemonių planas	Dokumentas, kuriame nurodytos tik tos Bendrovės rizikos, kurioms yra taikomos papildomos rizikų valdymo priemonės, nenumatytos jokiuose kituose Bendrovės dokumentuose.
Suinteresuota šalis (-ys)	Fizinis, juridinis asmuo ar jų grupės, organizacijos, institucijos ar įstaigos (bet kokios juridinės formos, neatsižvelgiant į jų naudos gavėjus), turintys skirtingus lūkesčius, poreikius ar įtaką Bendrovės ar jos veiklos atžvilgiu.
TIS2	Europos parlamento ir tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti, kuria iš dalies keičiamas Reglamentas (ES) Nr. 910/2014 ir Direktyva (ES) 2018/1972 ir panaikinama Direktyva (ES) 2016/1148.
Vientisumas	Informacijos savybė, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

2. BENDOSIOS NUOSTATOS

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

2.2. Bendrovės informacijos saugumo reikalavimų įgyvendinimas užtikrinamas ir valdomas nuosekliai planuojant, įgyvendinant, vertinant ir tobulinant ISVS, vadovaujantis ISO 27001, TIS2 ir kitais Europos Sąjungos, Lietuvos Respublikos teisės aktų reikalavimais.

2.3. Ši Politika reglamentuoja pagrindinius reikalavimus, kuriais vadovaujantis turi būti užtikrintas tinkamas ir efektyvus informacijos saugumo valdymas, išvengta veiklos sutrikdymo bei žalos atsiradimo dėl informacijos konfidencialumo, vientisumo, prieinamumo pažeidimų bei kitų kibernetinių grėsmių.

2.4. Politika taikoma Bendrovės suinteresuotoms šalims, taikoma procesuose, kur yra užtikrinamas informacijos saugumas, valdoma ar tvarkoma informacija.

2.5. Politika paruošta vadovaujantis ISO 27001 standarto reikalavimais ir kitų teisės aktų nustatytais informacijos saugumo reikalavimais.

3. INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI

3.1. Informacijos saugumas apima tris pagrindinius aspektus:

3.1.1. Informacijos konfidencialumą;
3.1.2. Informacijos vientisumą;
3.1.3. Informacijos prieinamumą.

3.2. Informacijos konfidencialumą, vientisumą ir prieinamumą užtikrina ISVS, kuri užtikrina, kad rizikos, susijusios su informacijos saugumu Bendrovėje būtų tinkamai valdomos.

3.3. Reikalavimai informacijos saugumui nustatomi vadovaujantis:
3.3.1. TIS2 ir kitais Europos Sąjungos, Lietuvos Respublikos teisės aktuose nustatytais informacijos saugumo reikalavimais;
3.3.2. Bendrovės strateginiais tikslais;
3.3.3. Atsižvelgiant į suinteresuotų šalių keliamus reikalavimus bei lūkesčius, išreikštus informacijos saugumą reglamentuojančiuose teisės aktuose, duomenų teikimo, tvarkymo ar kitokio pobūdžio su informacijos saugumo užtikrinimu susijusiose sutartyse, išoriniais ir vidiniais informacijos keitimosi būdais;
3.3.4. Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ir kituose teisinę galią turinčiuose dokumentuose;
3.3.5. Vertinant Bendrovės informacinių išteklių informacijos saugumo rizikas.

3.4. Bendrovė įsipareigoja:
3.4.1. Laikytis visų informacijos saugumo įsipareigojimų, reglamentuotų TIS2 ir kitų Europos Sąjungos, Lietuvos Respublikos teisės aktuose bei sutartyse;
3.4.2. Nustatyti ISVS tikslus, tobulinimo uždavinius ir priemones, įtraukiant juos į veiklos planus;
3.4.3. Užtikrinti efektyvų ISVS aprūpinimą reikiamais ištekliais;
3.4.4. Vystyti Informacijos saugumo kultūrą, sudaryti sąlygas Bendrovės darbuotojams tobulinti žinias informacijos saugumo srityje;
3.4.5. Nuosekliai gerinti Politiką, ISVS tikslus, atliekant ISVS vidaus auditus, nustatant neatitiktis, vykdant ISVS korekcinius veiksmus ir atliekant vadovybės vertinimo analizę.

3.5. Bendrovės reikalavimai taikomi:
3.5.1. Visuose Bendrovės veiklos procesuose, susijusiuose su informacijos saugumu bei saugiu informacijos tvarkymu;
3.5.2. Visai Bendrovės informacijai, nepriklausomai nuo jos formos ir saugojimo būdo;
3.5.3. Visoms Bendrovės suinteresuotoms šalims, kuriems teisės aktų ir (ar) sutartinių santykių pagrindu yra suteikta prieiga prie Bendrovės informacinių išteklių teisės aktuose ar sutartyje numatytoms funkcijoms (teisėms) atlikti;
3.5.4. Išorinių paslaugų teikėjų teikiamoms paslaugoms.

3.6. Bet koks Informacijos saugumo reikalavimų pažeidimas laikomas Informacijos saugumo incidentu, kuris gali daryti neigiamą įtaką Bendrovės veiklos tęstinumui, sugadinti ir pakenkti Bendrovės įvaizdžiui visuomenėje.

3.7. Bendrovės suinteresuotosioms šalims, pažeidus ISVS reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės.

4. INFORMACIJOS SAUGUMO VALDYMO SISTEMOS TIKSLAI:

4.1. apsaugoti visą informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos Bendrovės vykdomai veiklai ir įvaizdžiui;
4.2. užtikrinti ir valdyti informacijos saugumą, atsižvelgiant į Bendrovės veiklos strateginius tikslus;
4.3. užtikrinti ir valdyti atitikimą išoriniams ir vidiniams informacijos saugumo reikalavimams, atliekant periodinį atitikties vertinimą ir šalinant nustatytus trūkumus;
4.4. užtikrinti informacijos saugos incidentų sprendimą, jų priežasčių nustatymą ir pašalinimą, įgyvendinant informacijos saugos incidentų valdymo procesą;
4.5. užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant įgyvendinti Rizikų valdymo priemonių planą ir suvaldyti rizikas iki priimtino lygio;

4.6. užtikrinti tinkamą informacijos saugumo ir apdorojimo priemonių parinkimą ir įgyvendinimą, atliekant kasmetinį rizikos vertinimą;
4.7. užtikrinti reikiamų informacijos saugumo valdymo priemonių įgyvendinimą ir jų veiksmingumą;
4.8. užtikrinti veiklos tęstinumo valdymo / atstatymo planų tinkamumą, atliekant jų periodinius peržiūrą ir testavimą;
4.9. įgyvendinti TIS2 ir kituose Europos Sąjungos, Lietuvos Respublikos teisės aktuose nustatytus informacijos saugumo reikalavimus, vadovautis ISO 27001 standarto reikalavimais.

5. INFORMACIJOS SAUGUMO DALYVIŲ ATSAKOMYBĖS

Informacijos saugumo dalyviai	Pagrindinės atsakomybės ir funkcijos
Valdyba	- Tvirtina Politiką ir stebi jos įgyvendinimą; - Priima sprendimus keisti / atnaujinti / papildyti Politiką.
Audito komitetas	- Teikia pastabas / pasiūlymus / pastebėjimus dėl Politikos nuostatų keitimo / atnaujinimo / papildymo; - Teikia pastabas ir pasiūlymus dėl ISVS veiksmingumo ir efektyvumo.
Vidaus audito skyrius	- Atlieka patikrinimus dėl Politikos nuostatų tinkamo įgyvendinimo; - Vertina, nagrinėja, analizuoja ISVS įgyvendinimą bei teikia rekomendacijas, siūlymus ir pastabas dėl vidaus auditų metu nustatytų trūkumų, rekomendacijų ar pastebėjimų išsprendimo.
Generalinis direktorius	- Skiria reikiamą dėmesį ir užtikrina, kad būtų pakankamai žmogiškųjų, informacinių technologijų ir kitų išteklių informacijos saugumui užtikrinti; - Paskiria už informacijos saugą atsakingą darbuotoją / darbuotojus, kuris / kurie būtų atsakingas / atsakingi už Politikos ir joje iškeltų tikslų įgyvendinimą ir priežiūrą; - Užtikrina, kad ISVS sistema veiktų efektyviai ir tinkamai, nuolatos tobulina / gerina ISVS periodiškai peržiūrint ISVS tikslus; - Skatina ir įpareigoja laikytis informacijos saugumo reikalavimų; - Numato atsakomybę už informacijos saugumo reikalavimų nesilaikymą.
Struktūrinių padalinių vadovai	- Užtikrina informacijos saugumo laikymosi kontrolę padalinyje.
IT saugos įgaliotinis	- Vykdo Bendrovės informacinių sistemų saugos įgaliotinio funkcijas; - Rengia Politiką, esant poreikiui atlieka Politikos pakeitimus bei teikia juos tvirtinimui; - Teikia metodinę pagalbą informacijos saugumo klausimais; - Yra atsakingas už ISVS diegimą ir palaikymą bei informacijos saugumo organizavimą Bendrovėje; - Informuoja Nacionalinį kibernetinio saugumo centrą apie informacijos saugos incidentus, kurie daro įtaką Bendrovės veiklai; - Vykdo kitas pareigybės aprašyme ir kituose teisės aktuose nustatytas funkcijas.
IT skyriaus vadovas	- Techninių kibernetinio saugumo reikalavimų priemonių įgyvendinimo kontrolė.
Informacinės saugos ekspertas	- Techninių kibernetinio saugumo reikalavimų priemonių įgyvendinimas.
Suinteresuotos šalys	- Laikosi Politikos, susijusių išorinių ir Bendrovės teisės aktų, kitų dokumentų (pvz., sutarčių) reglamentuojančių / nustatančių informacijos saugumą, reikalavimų;

Informacijos saugumo dalyviai	Pagrindinės atsakomybės ir funkcijos
	- Įsipareigoja laikytis konfidencialumo reikalavimų; - Saugo jiems patikėtus informacinius išteklius, patikėtą Bendrovės informaciją, techninę ir programinę įrangą; - Informacinius išteklius naudoja tik su darbo santykiais susijusiais tikslais ir tik suteiktų įgaliojimų ribose, išskyrus jeigu kitaip reglamentuota susijusiuose Bendrovės teisės aktuose; - Nedelsdami praneša apie pastebėtus galimus ar įvykusius informacijos saugos įvykius ir incidentus IT saugos įgaliotiniui ir (arba) el. paštu cert@vv.lt.

6. BAIGIAMOSIOS NUOSTATOS

6.1. Politika tvirtinama ir keičiama Bendrovės valdybos sprendimu.
6.2. Su Politika yra supažindinamos Bendrovės suinteresuotos šalys.
6.3. Politika peržiūrima bent kartą per metus, atnaujinama – ne rečiau kaip kas treji (3) metai.
6.4. Už Politikos įgyvendinimą atsakingas Veiklos atsparumo skyriaus vadovas.
6.5. Politika yra skelbiama viešai Bendrovės interneto svetainėje adresu www.vv.lt.