|  |
| --- |
|  **UAB „Vilniaus vandenys“ kibernetinio ir informacijos saugumo politika**  |
| **Tikslas** | Kibernetinio ir informacijos saugumo politika (toliau – Politika) yra skirta nustatyti UAB „Vilniaus vandenys“ kibernetinio ir informacijos saugumo valdymo principus, nustatyti efektyvias saugumo užtikrinimo kryptis siekiant suvaldyti kibernetinių grėsmių informacijos saugos rizikas, bei teisės aktų atitiktį. |
| **Taikymo sritis** | Visi Bendrovės darbuotojai. |
| **Susiję teisės aktai**  | 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“ informacinių sistemų saugos politika;Informacinių sistemų (IS) naudotojų administravimo taisyklės;UAB „Vilniaus vandenys“ IT įrangos ir informacinių sistemų elektroninės informacijos naudojimo tvarkos aprašasInformacijos saugumo incidentų valdymo planas ir informacinių sistemų veiklos atkūrimo detalusis planas;UAB „Vilniaus vandenys“ fizinis ir veiklos apsaugos reglamentas;Informacinių ir komunikacinių technologijų naudojimo ir darbuotojų stebėsenos tvarkos aprašas;UAB „Vilniaus vandenys“ veiklos strategijos dokumentas. |
| **Nuorodos** | Lietuvos Respublikos kibernetinio saugumo įstatymas;Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;Lietuvos standartas LST ISO/IEC 27001:2017 „Informacijos technologija. Saugumo metodai. Informacijos saugumo valdymo praktikos kodeksas“;Lietuvos standartas LST ISO/IEC 27002:2017 „Informacinės technologijos. Saugumo metodai. Informacijos saugumo kontrolės priemonių praktikos nuostatai“. |

# Turinys

* + - 1. SPECIALIOSIOS SĄVOKOS IR SUTRUMPINIMAI
			2. BENDOSIOS NUOSTATOS
			3. INFORMACIJOS IR KIBERENTINĖS SAUGOS UŽTIKRINIMO PRINCIPAI
			4. INFORMACIJOS IR KIBERENTINĖS SAUGOS DALYVIŲ ATSAKOMYBĖS
			5. BAIGIAMOSIOS NUOSTATOS
1. **SPECIALIOSIOS SĄVOKOS IR SUTRUMPINIMAI**

|  |  |
| --- | --- |
| **Bendrovė**  | UAB „Vilniaus vandenys“ |
| **Rizikų valdymo priemonių planas** | Dokumentas, kuriame nurodytos tik tos Bendrovės rizikos, kurioms yra taikomos papildomos rizikų valdymo priemonės, nenumatytos jokiuose kituose Bendrovės dokumentuose. |
| **Informacija** | Bet koks žinių elementas, pateiktas tinkama naudoti, saugoti, perduoti ar apdoroti forma. Informacija apima žodine, rašytine, audiovizualine, skaitmenine ar bet kokia kita forma išreikštus ir apibendrintus arba interpretuotus duomenis. |
| **Informacijos saugumas** | Informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas. Kai tai tikslinga, papildomai gali būti įtraukti ir kiti kriterijai, tokie kaip atsakingumas, apskaita, autentiškumas, patikimumas, nepaneigiamumas ir privatumas. |
| **Informacinė sistema** | Informacijos apdorojimo sistemos ir organizacijos išteklių (pačios informacijos, žmonių, techninių priemonių, finansų ir pan.) visuma, skirta informacijai apdoroti, formuoti (kurti), skleisti (siųsti ir gauti). Tai struktūrizuotas procesų ir procedūrų rinkinys, kuriame yra kaupiami duomenys, organizuojami ir perduodami vartotojui. |
| **ISVS** | Informacinio saugumo valdymo sistema. |
| **Kibernetinis saugumas** | Visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę ryšių ir informacinėmis sistemomis perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, ryšių ir informacinių sistemų netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę ryšių ir informacinių sistemų veiklą. |
| **Politika** | UAB „Vilniaus vandenys“ kibernetinio ir informacijos saugumo politika. |
| **Vientisumas** | Užtikrinimas, kad informacija ir duomenys yra teisingi, nėra atsitiktinai ar neteisėtai pakeisti ir sunaikinti. Duomenys dažniausiai suklastojami dėl kenkimo programinės įrangos ar neteisėto užvaldymo, techninės ar programinės įrangos gedimo. |
| **Trečioji šalis** | Juridinis arba fizinis asmuo, kuriam suteikiama prieiga prie Bendrovės informacijos ar turto. |

1. **BENDOSIOS NUOSTATOS**
	1. Ši Politika reglamentuoja pagrindinius reikalavimus, kuriais vadovaujantis turi būti užtikrintas tinkamas ir efektyvus informacijos ir kibernetinio saugumo valdymas, išvengta veiklos sutrikdymo bei žalos atsiradimo dėl informacijos konfidencialumo, vientisumo, prieinamumo pažeidimų bei kitų kibernetinių grėsmių.
	2. Politika taikoma Bendrovės darbuotojams, tiekėjams bei rangovams ir taikoma procesuose, kur yra užtikrinamas informacijos ir kibernetinis saugumas, valdoma ar tvarkoma informacija.
	3. Politika paruošta vadovaujantis EN ISO/IEC 27001:2017 standarto reikalavimais ir kitų teisės aktų nustatytais informacijos saugos, kibernetinio saugumo ir asmens duomenų saugumo reikalavimais.
2. **KIBERENTINIO IR INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI**
	1. Informacijos saugumas apima tris pagrindinius aspektus:
		1. Informacijos konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo (informacija gali būti prieinama ar pateikiama tik įgaliotiems fiziniams ar juridiniams asmenims);
		2. Informacijos vientisumą – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo ar sunaikinimo;
		3. Informacijos prieinamumą – užtikrinimą, kad informacija prieinama tada, kai ji yra reikalinga.
	2. Informacijos konfidencialumą, vientisumą ir prieinamumą užtikrina ISVS, kuri užtikrina, kad rizikos, susijusios su informacijos saugumu Bendrovėje būtų tinkamai valdomos.
	3. Reikalavimai kibernetiniam ir informacijos saugumui nustatomi vadovaujantis:
		1. Europos Sąjungos ir Lietuvos Respublikos teisės aktuose nustatytais kibernetinio ir informacijos saugumo bei asmens duomenų saugumo reikalavimais;
		2. Bendrovės strateginiais tikslais;
		3. Atsižvelgiant į suinteresuotų šalių keliamus reikalavimus bei lūkesčius, išreikštus kibernetinį ir informacijos saugumą reglamentuojančiuose teisės aktuose, duomenų teikimo, tvarkymo ar kitokio pobūdžio su informacijos saugumo užtikrinimu susijusiose sutartyse, išoriniais ir vidiniais informacijos keitimosi būdais;
		4. Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ir kituose teisinę galią turinčiuose dokumentuose;
		5. Vertinant informacijos ir kibernetinio saugumo riziką.
	4. Informacijos ir kibernetinio saugumo valdymo prioritetinės kryptys:
		1. užtikrinti tinkamą ir efektyvų informacijos bei kibernetinio saugumo valdymą ir išvengti veiklos sutrikdymo dėl informacijos konfidencialumo, vientisumo bei prieinamumo pažeidimų;
		2. užtikrinti atitiktį teisės aktuose nustatytiems kibernetinio ir informacijos saugumo reikalavimams;
		3. įgyvendinti gerąją praktiką atitinkančias organizacines ir technines informacijos saugumo priemones;
		4. užtikrinti valdomų informacinių sistemų veiklos tęstinumą;
		5. užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant suvaldyti riziką iki priimtino lygio.
	5. Bendrovė įsipareigoja:
		1. Laikytis visų kibernetinio ir informacijos saugumo įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse;
		2. Nustatyti kibernetinio ir informacijos saugumo valdymo tikslus, tobulinimo uždavinius ir priemones, įtraukiant juos į veiklos planus;
		3. Užtikrinti efektyvų ISVS aprūpinimą reikiamais ištekliais;
		4. Vystyti Informacijos saugumo kultūrą, sudaryti sąlygas Bendrovės darbuotojams tobulinti žinias kibernetinio ir informacijos saugumo bei asmens duomenų saugumo srityse.
		5. Nuosekliai gerinti ISVS įgyvendinamo Politiką, kibernetinio ir informacijos saugumo valdymo tikslus, atliekant ISVS vidaus auditus, nustatant neatitiktis, vykdant ISVS korekcinius veiksmus ir atliekant vadovybės vertinimo analizę.
	6. Bendrovės reikalavimai taikomi:
		1. Visuose Bendrovės veiklos procesuose, susijusiuose su kibernetiniu saugumu bei saugiu informacijos tvarkymu;
		2. Visai Bendrovės informacijai, nepriklausomai nuo jos formos ir saugojimo būdo;
		3. Visiems Bendrovės darbuotojams ir Tretiesiems asmenims, kuriems teisės aktų ir (ar) sutartinių santykių pagrindu yra suteikta prieiga prie Bendrovės informacijos ar informacijos apdorojimo priemonių teisės aktuose ar sutartyje numatytoms funkcijoms (teisėms) atlikti;
		4. Išorinių paslaugų teikėjų teikiamoms paslaugoms.
	7. Bet koks Informacijos saugumo normų pažeidimas laikomas Informacijos saugumo incidentu, kuris gali daryti neigiamą įtaką Bendrovės veiklos tęstinumui, sugadinti ir pakenkti organizacijos įvaizdžiui visuomenėje.
	8. Bendrovės darbuotojams ir Trečiosioms šalims, pažeidusiems ISVS reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės.
3. **INFORMACIJOS IR KIBERENTINĖS SAUGOS DALYVIŲ ATSAKOMYBĖS**

| **Kibernetinio saugumo ir informacijos saugumo dalyviai** | **Pagrindinės atsakomybės ir funkcijos** |
| --- | --- |
| **Valdyba** | * Tvirtina Politiką;
* Priima sprendimus keisti / atnaujinti / papildyti Politiką;
 |
| **Audito komitetas** | * Teikia pastabas / pasiūlymus / pastebėjimus dėl Politikos nuostatų keitimo / atnaujinimo / papildymo;
* Teikia pastabas ir pasiūlymus dėl kibernetinio saugumo ir informacijos saugumo sistemos veiksmingumo ir efektyvumo.
 |
| **Vidaus audito skyrius** | * Atlieka patikrinimus dėl Politikos nuostatų tinkamo įgyvendinimo;
* Vertina, nagrinėja, analizuoja kibernetinio saugumo ir informacijos saugumo sistemos įgyvendinimą bei teikia rekomendacijas, siūlymus ir pastabas dėl vidaus auditų metu nustatytų trūkumų, rekomendacijų ar pastebėjimų išsprendimo.
 |
| **Generalinis direktorius** | * Užtikrina, kad būtų skiriama pakankamai žmogiškųjų, informacinių technologijų ir kitų išteklių kibernetinio saugumo ir informacijos saugumui užtikrinti;
* Užtikrina, kad ISVS sistema veiktų efektyviai ir tinkamai;
* Skatina ir įpareigoja Darbuotojus laikytis kibernetinio saugumo ir informacijos saugumo reikalavimų.
 |
| **Struktūrinių padalinių vadovai** | * Užtikrina kibernetinio saugumo ir informacijos saugumo laikymosi kontrolę padalinyje;
* Užtikrina, kad padalinyje būtų laikomasi pagrindinių kibernetinio saugumo ir informacijos saugumo reikalavimų;
* Yra atsakingi už jiems pavaldžių Darbuotojų veiksmus dėl kibernetinio saugumo ir informacijos saugumo.
 |
| **IT skyriaus vadovas** | * Rengia Politiką;
* Esant poreikiui atlieka Politikos pakeitimus bei teikia juos tvirtinimui;
* Teikia metodinę pagalbą kibernetinio saugumo ir informacijos saugumo klausimais Darbuotojams;
* Yra atsakingas už ISVS diegimą ir palaikymą bei kibernetinį saugumą ir informacijos saugumą Bendrovėje.
* Teikia informaciją apie kibernetinio saugumo ir informacijos saugumo incidentus, kurie daro Bendrovės veiklai.
 |
| **Darbuotojai** | * Kiekvienas Darbuotojas kasdienėje veikloje užtikrina savo funkcijų ir atliekamų veiksmų atitikimą kibernetinio saugumo ir informacijos saugumo reikalavimams;
* Nedelsiant informuoja apie pastebėtus kibernetinio saugumo ir informacijos saugumo incidentus;
* Teikia pasiūlymus dėl kibernetinio saugumo ir informacijos saugumo gerinimo Bendrovėje.
 |

1. **BAIGIAMOSIOS NUOSTATOS**
	1. Politika tvirtinama ir keičiama Bendrovės valdybos sprendimu.
	2. Su Politika yra supažindinami priimami ir esami Bendrovės darbuotojai, visi tiekėjai bei rangovai.
	3. Politika peržiūrima ne rečiau kaip kas treji (3) metai.
	4. Politika yra skelbiama viešai Bendrovės interneto svetainėje adresu www.vv.lt.