INFORMACIJOS SAUGUMO POLITIKA

Tikslas	Informacijos saugumo politika (toliau – Politika) nustato UAB „Vilniaus vandenys“ informacijos ir kibernetinio saugumo valdymo principus bei pagrindines kryptis, siekiant valdyti saugumo rizikas, užtikrinti Bendrovės veiklos atsparumą ir atitiktį taikomiems teisės aktų bei ISO 27001 standarto reikalavimams.
Taikymo sritis	Politika taikoma visai UAB „Vilniaus vandenys“ veiklai, darbuotojams, informaciniams ištekliams, informacinėms sistemoms ir IT bei technologinei (OT) infrastruktūrai. Politikos reikalavimai taip pat taikomi tretiesiems asmenims tiek, kiek jiems suteikiama prieiga prie Bendrovės informacijos, informacinių sistemų ar infrastruktūros arba jie teikia su jomis susijusias paslaugas.
Susiję teisės aktai	Politika taikoma vadovaujantis teisės aktais ir Bendrovės vidaus dokumentais, reglamentuojančiais kibernetinį ir informacijos saugumą, asmens duomenų apsaugą, dirbtinio intelekto naudojimą ir informacinių technologijų valdymą. *Europos Sąjungos teisės aktai:* • 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas – BDAR); • 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 teisės aktai:* • Lietuvos Respublikos kibernetinio saugumo įstatymas; • Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas; • Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas; • Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“. *Standartai:* • Standartas LST EN ISO/IEC 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga – Informacijos saugumo valdymo sistemos – Reikalavimai“; • Standartas LST EN ISO/IEC 27002:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga – Informacijos saugumo kontrolės priemonės“. *Savivaldybės dokumentai:*

	• Vilniaus miesto savivaldybės administracijos ir savivaldybės kontroliuojamų įmonių ir įstaigų bendroji informacijos saugumo politika, patvirtinta Vilniaus miesto savivaldybės mero 2025 m. birželio 18 d. potvarkiu Nr. 955-996/25. *Bendrovės vidaus dokumentai:* • Informacinių sistemų duomenų saugos nuostatai; • Konfidencialios informacijos valdymo politika; • Konfidencialios informacijos valdymo taisyklės; • Suinteresuotų šalių įtraukimo politika; • Asmens duomenų tvarkymo ir saugumo politika; • Asmens duomenų tvarkymo ir saugumo politikos įgyvendinimo taisyklės; • Rizikų valdymo politika; • Veiklos tęstinumo politika; • Generatyvinio dirbtinio intelekto naudojimo politika; • Generatyvinio dirbtinio intelekto naudojimo gairės; • Informacijos saugumo valdymo sistemos vadovas.
Savininkas	Veiklos atsparumo skyriaus vadovas.
Pirminės politikos sukūrimo data	2022-01-13 Valdybos posėdžio protokolas Nr. PR-V22-1.

TURINYS

1. SĄVOKOS IR SUTRUMPINIMAI 2
2. BENDRIEJI REIKALAVIMAI 4
3. ĮGYVENDINIMO PRINCIPAI 4
4. POLITIKOS ĮGYVENDINIMAS 6
5. POLITIKOS STEBĖSENA 9
6. BAIGIAMOSIOS NUOSTATOS 9

1. SĄVOKOS IR SUTRUMPINIMAI

Sąvoka/Sutrumpinimas	Paaiškinimas
Atitikties vertinimas	Informacinių technologijų saugos atitikties vertinimas organizacinių ir techninių kibernetinio saugumo reikalavimų pagal Lietuvos Respublikos kibernetinio saugumo įstatymą ir jį įgyvendinančius teisės aktus.
Bendrovė	UAB „Vilniaus vandenys“.
BDAR	2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas).
CISO	Kibernetinio saugumo vadovas (angl. *Chief Information Security Officer*).

ESOC	Ekstremaliųjų situacijų operacijų centras.
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, neišsižadėjimas 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 LST EN ISO/IEC 27001:2023 „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.
ISVG	Bendrovės generalinio direktoriaus įsakymu sudaryta darbuotojų informacijos saugumo valdymo grupė, kuri vykdo šioje Politikoje ir kituose ISVS dokumentuose priskirtas funkcijas.
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.
KSIS	Kibernetinio saugumo informacinė sistema, administruojama Nacionalinio kibernetinio saugumo centro prie Krašto apsaugos ministerijos.
Konfidencialumas	Informacijos savybė, reiškianti, kad su informacija gali susipažinti tik įgalioti asmenys.
NKSC	Nacionalinis kibernetinio saugumo centras prie Krašto apsaugos ministerijos.
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.
SOC	Saugumo operacijų centras.
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. BENDRIEJI REIKALAVIMAI

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 standarto 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 standarto ISO 27001 reikalavimais ir kitų teisės aktų nustatytais informacijos saugumo reikalavimais.

3. ĮGYVENDINIMO 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. Bendrovės informacijos saugumas grindžiamas šiais kibernetinio saugumo principais, kurie turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiant pirmenybės:

3.2.1. Kibernetinės erdvės nediskriminavimo – teisės aktų nuostatos yra taikomos, o teisės aktų saugomų gėrių apsauga yra užtikrinama vienodai tiek fizinėje, tiek kibernetinėje erdvėje;

3.2.2. Kibernetinio saugumo rizikos valdymo – taikomos kibernetinio saugumo rizikos valdymo priemonės turi užtikrinti Bendrovės reguliariai įvertinamos rizikos suvaldymą;

3.2.3. Kibernetinio saugumo proporcingumo – taikomos kibernetinio saugumo rizikos valdymo priemonės neturi apriboti Bendrovės veiklos labiau, negu tai būtina kibernetiniam saugumui užtikrinti. Rizikos valdymo priemonės parenkamos įvertinus jų ekonominį naudingumą ir priimtiną riziką, kurią Bendrovė sutinka prisiimti, atsižvelgiant į veiklos kontekstą bei kritinės veiklos tęstinumo poreikius;

3.2.4. Viešojo intereso viršenybės – taikomos kibernetinio saugumo rizikos valdymo priemonės pirmiausia turi užtikrinti viešojo intereso apsaugą, tačiau neturi iš esmės pažeisti atskirų vartotojų, Bendrovės teisių ir teisėtų interesų ar neproporcingai apriboti jų laisvės;

3.2.5. Standartizacijos ir technologinio neutralumo – įgyvendinant kibernetinio saugumo rizikos valdymo priemones, Bendrovė skatinama vadovautis nacionaliniais, Europos Sąjungos ir kitais tarptautiniais tinklų ir IS saugumo standartais ir techninėmis specifikacijomis, nereikalaujant taikyti kokios nors konkrečios rūšies technologijos ir nesuteikiant jai pirmenybės;

3.2.6. Subsidiarumo – už tinklų ir IS ir jomis teikiamų paslaugų kibernetinį saugumą yra atsakinga Bendrovė. Srityse, kurios priklauso išimtinei Bendrovės kompetencijai, NKSC veiksmų imasi tik tada, kai tinklų ir IS ir jomis teikiamų paslaugų kibernetinio saugumo neužtikrina Bendrovė.

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

3.4. Reikalavimai informacijos saugumui nustatomi vadovaujantis:

3.4.1. TIS2 ir kitais Europos Sąjungos, Lietuvos Respublikos teisės aktuose nustatytais informacijos saugumo reikalavimais;

3.4.2. Bendrovės strateginiais tikslais;

3.4.3. 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;

3.4.4. Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ir kituose teisinę galią turinčiuose dokumentuose;

3.4.5. Vertinant Bendrovės informacinių išteklių informacijos saugumo rizikas.

3.5. Bendrovė įsipareigoja:

3.5.1. Laikytis visų informacijos saugumo įsipareigojimų, reglamentuotų TIS2 ir kitų Europos Sąjungos, Lietuvos Respublikos teisės aktuose bei sutartyse;

3.5.2. Nustatyti ISVS tikslus, tobulinimo uždavinius ir priemones, įtraukiant juos į veiklos planus;

3.5.3. Užtikrinti efektyvų ISVS aprūpinimą reikiamais ištekliais;

3.5.4. Vystyti Informacijos saugumo kultūrą, sudaryti sąlygas Bendrovės darbuotojams tobulinti žinias informacijos saugumo srityje;

3.5.5. Nuosekliai gerinti Politiką, ISVS tikslus, atliekant ISVS vidaus auditus, nustatant neatitiktis, vykdant ISVS korekcinius veiksmus ir atliekant vadovybės vertinimo analizę.

3.6. Bendrovės reikalavimai taikomi:

3.6.1. Visuose Bendrovės veiklos procesuose, susijusiuose su informacijos saugumu bei saugiu informacijos tvarkymu;

3.6.2. Visai Bendrovės informacijai, nepriklausomai nuo jos formos ir saugojimo būdo;

3.6.3. 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;

3.6.4. Išorinių paslaugų teikėjų teikiamoms paslaugoms.

3.7. Bendrovės ISVS sertifikavimo sritis – „Vandens išgavimas, paruošimas ir tiekimas. Nuotekų surinkimas ir valymas. Su tuo susijusios papildomos komercinės paslaugos ir projektų valdymas“.

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

3.9. 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. POLITIKOS ĮGYVENDINIMAS

4.1. Politikos įgyvendinimas užtikrinamas per Bendrovės informacijos saugumo valdymo sistemą (ISVS), kurios tikslai yra:

4.1.1. apsaugoti visą informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos Bendrovės vykdomai veiklai ir įvaizdžiui;

4.1.2. užtikrinti ir valdyti informacijos saugumą, atsižvelgiant į Bendrovės veiklos strateginius tikslus;

4.1.3. užtikrinti ir valdyti atitikimą išoriniams ir vidiniams informacijos saugumo reikalavimams, atliekant periodinį ISVS vidaus auditą ir Atitikties vertinimą bei ISVS valdymo peržiūrą (vadovybės vertinamoji analizė), šalinant nustatytus trūkumus ir įgyvendinant gerinimo veiksmus;

4.1.4. užtikrinti informacijos saugos incidentų sprendimą, jų priežasčių nustatymą ir pašalinimą, įgyvendinant informacijos saugos incidentų valdymo procesą;

4.1.5. užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant įgyvendinti Rizikų valdymo priemonių planą ir suvaldyti rizikas iki priimtino lygio;

4.1.6. užtikrinti tinkamą informacijos saugumo ir apdorojimo priemonių parinkimą ir įgyvendinimą, atliekant kasmetinį rizikos vertinimą;

4.1.7. užtikrinti reikiamų informacijos saugumo valdymo priemonių įgyvendinimą ir jų veiksmingumą;

4.1.8. užtikrinti veiklos tęstinumo valdymo / atstatymo planų tinkamumą, atliekant jų periodinę peržiūrą ir testavimą;

4.1.9. įgyvendinti TIS2 ir kituose Europos Sąjungos, Lietuvos Respublikos teisės aktuose nustatytus informacijos saugumo reikalavimus, vadovautis standarto ISO 27001 reikalavimais.

4.2. Politikos įgyvendinime dalyvaujančių šalių atsakomybės:

Informacijos saugumo dalyviai	Pagrindinės atsakomybės ir funkcijos
Audito, rizikų ir tvarumo komitetas	- Teikia pastabas / pasiūlymus / pastebėjimus dėl Politikos nuostatų keitimo / atnaujinimo / papildymo; - Teikia pastabas ir pasiūlymus dėl ISVS veiksmingumo ir efektyvumo.
Duomenų apsaugos pareigūnas	- Pagal kompetenciją dalyvauja užtikrinant asmens duomenų apsaugos atitiktį taikomiems teisės aktams, įskaitant BDAR, Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymo reikalavimus ir kitus ISVS dokumentus.
ESOC	- Užtikrina veiklos tęstinumui kylančių grėsmių valdymą ir veiklų atkūrimo koordinavimą įvykus incidentui ir (ar) sutrikimui.
Fizinės saugos projektų vadovas	- Įgyvendina fizinės saugos reikalavimų atitikimo priemones, koordinuoja fizinės saugos valdymo procesą.

Informacijos saugumo dalyviai	Pagrindinės atsakomybės ir funkcijos
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.
Incidentų valdymo grupė ir (ar) SOC	- Valdo kibernetinius incidentus.
ISVG	- Peržiūri ISVS ketvirtinius rezultatus, įskaitant, tačiau neapsiribojant informacijos ir kibernetinio saugumo įvykių ir incidentų suvestinėmis ir jų valdymo rezultatais, ISVS procesų planavimo ir įgyvendinimo rezultatais, neatitikčių šalinimo ir korekcinių, rizikos valdymo ir ISVS gerinimo bei ISVS stebėjimo veiksmų rezultatais; - Prieš teikiant Bendrovės generaliniam direktoriui tvirtinti, peržiūri ir esant poreikiui koreguoja arba paveda atsakingiems Bendrovės darbuotojams pakoreguoti Informacijos saugumo rizikos vertinimo, Atitikties vertinimo, Veiklos atkūrimo planų išbandymų ir ISVS vidaus auditų rezultatus, taip pat Veiklos tęstinumo ir veiklos atkūrimo planų išbandymo plano, Informacijos saugumo rizikos vertinimo plano, Bendrovės darbuotojų ugdymo plano ir kitų planų projektus; - Peržiūri suplanuotas ISVS veiklas, pagal poreikį keičia jų įgyvendinimo prioritetus; - Teikia Bendrovės generaliniam direktoriui konsultacijas informacijos ir kibernetinio saugumo valdymo, ISVS palaikymo ir gerinimo klausimais.
IT skyriaus vadovas	- Užtikrina techninių kibernetinio saugumo reikalavimų priemonių įgyvendinimo kontrolę.
Kibernetinės saugos ekspertas / Kibernetinio saugumo inžinierius	- Įgyvendina techninių kibernetinio saugumo reikalavimų priemones.
Kibernetinio saugumo vadovas (CISO)	- Vykdo Bendrovės kibernetinio saugumo vadovo funkcijas; - Iki atskiro Saugos įgaliotinio paskyrimo vykdo Bendrovės Saugos įgaliotinio funkcijas; - Vykdo Vadovybės atstovo ISVS funkcijas; - Rengia Politiką, esant poreikiui atlieka Politikos pakeitimus bei teikia juos tvirtinimui;

Informacijos saugumo dalyviai	Pagrindinės atsakomybės ir funkcijos
	- Organizuoja Bendrovės Atitikties vertinimą, rizikos vertinimą ir veiklos tęstinumo valdymo plano (-ų) išbandymo pratybas, teikia rezultatus tvirtinimui ir Lietuvos Respublikos kibernetinio saugumo įstatymo nustatyta tvarka ir terminais pateikia NKSC į KSIS; - Teikia metodinę pagalbą informacijos saugumo klausimais; - Informuoja NKSC apie informacijos saugos incidentus, kurie daro įtaką Bendrovės veiklai; - Organizuoja darbuotojų mokymus informacijos saugumo klausimais; - Teikia administratoriams ir (ar) IS naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Politika ir kitų ISVS dokumentuose nustatytų reikalavimų įgyvendinimu; - Vykdo kitas pareigybės aprašyme ir kituose teisės aktuose nustatytas funkcijas.
Rizikų valdymo vadovas	- Koordinuoja rizikų valdymo procesą.
Saugos įgaliotinis	- Vykdo teisės aktuose ir Bendrovės vidaus teisės aktuose Saugos įgaliotiniui nustatytas funkcijas.
Struktūrinių padalinių vadovai	- Užtikrina informacijos saugumo laikymosi kontrolę padalinyje.
Suinteresuotosios šalys	- Laikosi Politikos, susijusių išorinių ir Bendrovės teisės aktų, kitų dokumentų (pvz., sutarčių) reglamentuojančių / nustatančių informacijos saugumą, reikalavimų; - 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 el. paštu cert@vv.lt.
Vadovų taryba	- Teikia pastabas / pasiūlymus / pastebėjimus dėl Politikos nuostatų keitimo / atnaujinimo / papildymo; - Teikia pastabas ir pasiūlymus dėl ISVS veiksmingumo ir efektyvumo.
Vadovybės atstovas ISVS	- Užtikrina ISVS suderinimą su Bendrovės tikslais ir strategija; - Komunikuoja apie ISVS strateginiame ir operatyviniame lygmenyje, įtraukiant Bendrovės darbuotojus į ISVS įgyvendinimą; - Prižiūri Politiką ir kitų ISVS dokumentų valdymą ir reikalavimų įgyvendinimą;

Informacijos saugumo dalyviai	Pagrindinės atsakomybės ir funkcijos
	- Koordinuoja ISVS vidaus auditus, pagal poreikį gali juose tiesiogiai dalyvauti, kaip vidaus auditorius, audito grupės vadovas arba koordinuoti išorės (konsultacinės ar sertifikavimo įmonės) auditoriams atliekant ISVS auditus; - Užtikrina ISVS atitiktį standarto ISO 27001 reikalavimams; - Įgyvendina Politikoje numatytus ISVS tikslus; - Rengia ISVS neatitikčių šalinimo veiksmų planus; - Organizuoja ir veda ISVG posėdžius; - Teikia Bendrovės vadovybei ataskaitas apie ISVS veiksmingumą ir galimus gerinimus bei organizuoja ISVS valdymo peržiūrą (vadovybės vertinamoji analizė); - Užtikrina, kad būtų identifikuojamos, vertinamos ir valdomos su informacijos saugumu susijusios rizikos bei koordinuoti rizikos mažinimo priemones; - Užtikrina, kad Bendrovės darbuotojai būtų tinkamai informuoti apie ISVS reikalavimus ir jų laikytųsi; - Atlieka kitas Politikoje ir ISVS dokumentuose bei Standarte ISO 27001 nustatytas funkcijas.
Valdyba	- Tvirtina Politiką ir stebi jos įgyvendinimą; - Priima sprendimus keisti / atnaujinti / papildyti Politiką.
Veiklos atsparumo skyriaus vadovas	- Užtikrina Politikos laikymosi kontrolę Bendrovėje. - Užtikrina Politikos nuostatų atitikties ir įgyvendinimo rezultatų surinkimą ir pateikimą generaliniam direktoriui.
Veiklos atkūrimo grupė	- Užtikrina veiklos atkūrimą ir veikimą įvykus incidentui ir (ar) sutrikimui.
Veiklos tęstinumo vadovas	- Koordinuoja veiklos tęstinumo valdymą.
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.

5. POLITIKOS STEBĖSENA

5.1. Politika peržiūrima esant pokyčiams, bet ne rečiau kaip kartą per 1 (vienerius) metus. Už Politikos peržiūrą ir atnaujinimą laiku atsakingas Kibernetinio saugumo vadovas (CISO).

5.2. Politikos laikymosi ir įgyvendinimo rezultatai ne rečiau kaip kartą per metus apibendrinami ir pateikiami Generaliniam direktoriui. Už Politikos laikymosi ir įgyvendinimo rezultatų surinkimą ir pateikimą atsakingas Veiklos atsparumo skyriaus vadovas.

6. BAIGIAMOSIOS NUOSTATOS

6.1. Politika tvirtinama ir keičiama Bendrovės Valdybos sprendimu.

6.2. Su Politika privalo susipažinti ir jos laikytis visi esami ir naujai priimami Bendrovės darbuotojai bei paskirti Valdybos nariai.

6.3. Asmenys, atstovaujantys Bendrovei ar veikiantys jos vardu, tačiau nesantys Bendrovės darbuotojais, turi būti supažindinti su Politika ir įsipareigoti jos laikytis.

6.4. Už Politikos įgyvendinimą atsakingas Generalinis direktorius.

6.5. Politika skelbiama Bendrovės interneto svetainėje.