PATVIRTINTA
Akcinės bendrovės „Regitra“
2025 m. rugsėjo 16 d.
valdybos posėdžio
protokolu Nr. 2V-5754

AKCINĖS BENDROVĖS „REGITRA“ INFORMACIJOS SAUGUMO POLITIKA

TURINYS

1. PAGRINDINĖS SĄVOKOS

AB „Regitra“	Akcinė bendrovė „Regitra“, juridinio asmens kodas 110078991
Atitikties vertinimas	Informacinių technologijų saugos atitikties vertinimas, atliekamas pagal Informacinių technologijų saugos atitikties vertinimo metodiką, patvirtintą Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“.
Kibernetinis saugumas	Visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, kuriomis siekiama išlaikyti atsparumą veiksniams, kibernetinėje erdvėje keliantiems grėsmę tinklų ir informacinėmis sistemomis (toliau – TIS) perduodamos ar jose tvarkomos elektroninės informacijos prieinamumui, autentiškumui, vientisumui ir konfidencialumui, TIS netrikdomam veikimui, valdymui arba paslaugų šiomis sistemomis teikimui, taip pat kuriomis siekiama atkurti įprastinę TIS veiklą.
Informacija	Visa AB „Regitra“ gaunama, siunčiama, kuriama, valdoma ir naudojama informacija, nepriklausomai nuo jos formos ir saugojimo būdo (rašytinė, skaitmeninė, elektroninė ir kt.).
Politika	Ši Akcinės bendrovės „Regitra“ informacijos saugumo politika.

Kitos šioje Politikoje vartojamos sąvokos suprantamos taip, kaip apibrėžiamos Lietuvos Respublikos kibernetinio saugumo įstatyme.

2. BENDROSIOS NUOSTATOS

2.1. Ši Politika yra pagrindinis AB „Regitra“ informacijos ir kibernetinio saugumo valdymą reglamentuojantis dokumentas, skirtas nustatyti AB „Regitra“ informacijos ir kibernetinio saugumo valdymo principus ir efektyvias saugumo užtikrinimo kryptis bei AB „Regitra“ prisiimtus įsipareigojimus, siekiant tinkamai valdyti informacijos ir kibernetinio saugumo rizikas bei užtikrinti tarptautinių ir Lietuvos Respublikos teisės aktų reikalavimų bei AB „Regitra“ prisiimtų įsipareigojimų informacijos ir kibernetinio saugumo srityje įgyvendinimą.

2.2. Šios Politikos tikslas – pateikti AB „Regitra“ valdybos poziciją informacijos ir kibernetinio saugumo atžvilgiu bei apsaugoti visą AB „Regitra“ informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos AB „Regitra“ vykdomai veiklai ir reputacijai. Informacija – tai strategiškai svarbus AB „Regitra“ veiklai turtas, todėl jos praradimas, neteisėtas pakeitimas, sugadinimas, atskleidimas ar informacijos apdorojimo nutraukimas gali sukelti AB „Regitra“ veiklos sutrikimus.

2.3. Ši Politika apima ir numato:

2.3.1. pagrindines gaires, kuriomis, siekiant apsaugoti AB „Regitra“ ir jos klientų informaciją, privalo vadovautis visi AB „Regitra“ darbuotojai, rangovai ir kitos susijusios šalys veikiančios asmenų, siekiančių įgyti ar susigrąžinti teisę vairuoti kelių transporto priemones, egzaminavimo (teorinių žinių, praktinių transporto priemonės valdymo įgūdžių ir gebėjimų patikrinimo), vairuotojo pažymėjimų, tarptautinių vairuotojo pažymėjimų ir vairuotojo kvalifikacijos kortelių išdavimo, transporto priemonių nuosavybės teisės deklaravimo, transporto priemonių registracijos mokesčio administravimo, transporto priemonių registravimo, valstybinio registracijos numerio ženklų išdavimo, registrų informacinių sistemų duomenų teikimo srityse bei kituose AB „Regitra“ veiklos procesuose, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo;

2.3.2. informacijos ir kibernetinio saugumo tikslus, kuriais siekiama apsaugoti AB „Regitra“ ir klientų informacijos konfidencialumą, vientisumą ir prieinamumą;

2.3.3. informacijos saugumo valdymo sistemos (toliau – ISVS) taikymo sritis;

2.3.4. informacijos ir kibernetinio saugumo principus;

2.3.5. AB „Regitra“ valdymo organų įsipareigojimus bei atsakomybes.

2.4. Ši Politika parengta vadovaujantis Lietuvos Respublikos kibernetinio saugumo įstatymu ir jo įgyvendinimą reglamentuojančių poįstatyminių teisės aktų reikalavimais, keliamais Tinklų ir informacinių sistemų kibernetinio saugumo politikai, taip pat Lietuvos standarto LST EN ISO/IEC ISO 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“ (toliau – Lietuvos standartas LST EN ISO/IEC ISO 27001) reikalavimais.

2.5. Tarptautiniai ir Lietuvos Respublikos teisės aktai bei standartai, kuriais turi būti vadovaujamasi įgyvendinant Politiką:

2.5.1. 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;

2.5.2. Lietuvos Respublikos kibernetinio saugumo įstatymas;

2.5.3. Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimas Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

2.5.4. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

2.5.5. Lietuvos standartas LST EN ISO/IEC ISO 27001;

2.5.6. Lietuvos standartas LST EN ISO/IEC 27002:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės“;

2.5.7. kitais teisės aktais, reglamentuojančiais informacijos ir kibernetinį saugumą.

2.6. Politikoje numatytiems tikslams įgyvendinti AB „Regitra“ yra įdiegta ir palaikoma ISVS, kuri turi atitikti naujausią Lietuvos standarto LST EN ISO/IEC 27001 leidimą.

2.7. Politikos nuostatos įgyvendinamos AB „Regitra“ vidaus teisės aktais, kuriuos tvirtina AB „Regitra“ vadovas (generalinis direktorius).

3. INFORMACIJOS IR KIBERNETINIO SAUGUMO PRINCIPAI

3.1. AB „Regitra“ informacijos saugumas grindžiamas kibernetinio saugumo principais, kurie numatyti Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje.

3.2. Taikant kibernetinį saugumą reglamentuojančias teisės normas, turi būti atsižvelgiama į visus Lietuvos Respublikos kibernetinio saugumo įstatymo 3 straipsnyje nurodytus principus. Šie principai turi būti derinami tarpusavyje, nė vienam iš jų iš anksto nesuteikiama pirmenybė.

4. ATSAKOMYBĖS

	Pagrindinės atsakomybės
Valdyba	– Tvirtindama šią Politiką nustato informacijos ir kibernetinio saugumo užtikrinimo kryptis, AB „Regitra“ siekius; – 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.

Generalinis direktorius	– Užtikrina, kad būtų skiriama pakankamai žmogiškųjų ir informacinių technologijų ir kitų išteklių informacijos ir kibernetinio saugumui užtikrinti; – Užtikrina, kad ISVS sistema veiktų efektyviai ir tinkamai bei būtų laiku peržiūrima ir tobulinama; – Skatina ir įpareigoja darbuotojus laikytis informacijos ir kibernetinio saugumo reikalavimų; – Sudaro sąlygas darbuotojams tobulinti savo žinias informacijos ir kibernetinio saugumo srityse.
Padalinių vadovai	– Užtikrina, kad informacijos ir kibernetinio saugumo reikalavimai būtų integruoti į veiklos procesus, o informacijos ir kibernetinio saugumo rizikos klausimus laiko neatsiejama savo veiklos dalimi; – Skiria tinkamą dėmesį ir išteklius informacijos ir kibernetinio saugumo užtikrinimui ir identifikuotų rizikų valdymui; – Užtikrina, kad padalinyje būtų laikomasi informacijos ir kibernetinio saugumo reikalavimų.
Informacijos ir kibernetinio saugumo funkcija	– Rengia Politiką, dalyvauja jos įgyvendinime; – Esant poreikiui atlieka Politikos pakeitimus bei teikia juos tvirtinimui; – Teikia pagalbą ir konsultacijas, organizuoja mokymus informacijos ir kibernetinio saugumo temomis bei organizuoja atsparumo patikras darbuotojams; – Užtikrina ISVS diegimą ir palaikymą AB „Regitra“; – Vertina kibernetines grėsmes, teikia informaciją apie informacijos saugumo ir kibernetinius incidentus teisės aktų nustatyta tvarka; – Atlieka kibernetinių incidentų valdymą; – Organizuoja ir (ar) vertina informacijos ir kibernetinio saugumo rizikas; – Teikia informaciją valdybai, audito komitetui ir generaliniam direktoriui apie ISVS būseną.
Paslaugų teikėjai	– Užtikrina, kad jų infrastruktūra ir procesai atitiktų jiems keliamus informacijos ir kibernetinio saugumo reikalavimus, atsako už jų laikymąsi ir saugų AB „Regitra“ informacinių išteklių naudojimą.
Darbuotojai	– Užtikrina informacijos ir kibernetinį saugumą kasdienėje veikloje priimdami sprendimus, suderintus su nuostatomis, reglamentuojančiomis kibernetinę ir informacijos saugą; – Nedelsiant informuoja apie pastebėtus informacijos saugumo ir kibernetinius incidentus; – Teikia pasiūlymus dėl informacijos ir kibernetinio saugumo gerinimo AB „Regitra“.

5. INFORMACIJOS IR KIBERNETINIO SAUGUMO TIKSLAI

5.1. Politika nustato šiuos informacijos ir kibernetinio saugumo tikslus:

5.1.1. užtikrinti ir valdyti informacijos ir kibernetinį saugumą, atsižvelgiant į AB „Regitra“ veiklos (strateginius) tikslus;

5.1.2. užtikrinti ir valdyti atitikimą išoriniams ir vidiniams informacijos ir kibernetinio saugumo reikalavimams, atliekant periodinį Politikos ir jos įgyvendinimą reglamentuojančių ISVS tvarkų peržiūrą ir šalinant nustatytus trūkumus;

5.1.3. užtikrinti informacijos saugumo pažeidimų ir kibernetinių incidentų valdymą ir jų priežasčių pašalinimą, įgyvendinant informacijos saugos ir kibernetinių incidentų valdymo procesą, taip pat teisės aktų nustatyta tvarka kontroliuojančioms institucijoms pranešti apie didelius kibernetinius incidentus;

5.1.4. užtikrinti tinkamą informacijos saugumo ir apdorojimo priemonių parinkimą bei įgyvendinimą, atliekant kasmetinį rizikos vertinimą ir įgyvendinant rizikų valdymo planą;

5.1.5. užtikrinti taikomų informacijos apsaugos priemonių veiksmingumą, atliekant ISVS vidaus auditą ir ISVS valdymo peržiūrą, siekiant pašalinti nustatytas ISVS neatitiktis ir įgyvendinti gerinimo veiksmus;

5.1.6. užtikrinti tarptautinių ir Lietuvos Respublikos teisės aktų, reglamentuojančių informacijos ir kibernetinio saugumo valdymą, reikalavimų atitiktį, atliekant atitikties vertinimus, siekiant pašalinti nustatytas neatitiktis ir įgyvendinti neatitikčių šalinimo veiksmus;

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

5.1.8. užtikrinti Politikos įgyvendinimui ir ISVS palaikymui būtinus žmogiškuosius, finansinius bei kitus išteklius;

5.1.9. užtikrinti darbuotojų dalyvaujančių informacijos ir kibernetinio saugumo valdyme bei ISVS palaikyme kompetencijos ir kvalifikacijos kėlimą.

5.2. Informacijos ir kibernetinis saugumas apima tris pagrindinius aspektus:

Konfidencialumą – informacijos apsaugą nuo nesankcionuoto atskleidimo	**Vientisumą –** informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo	**Prieinamumą –** užtikrinimą, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti AB „Regitra“ veiklą

5.3. **AB „Regitra“ ISVS taikymo sritis:** asmenų, siekiančių įgyti ar susigrąžinti teisę vairuoti kelių transporto priemones, egzaminavimas (teorinių žinių, praktinių transporto priemonės valdymo įgūdžių ir gebėjimų patikrinimas); Vairuotojo pažymėjimų, tarptautinių vairuotojo pažymėjimų ir vairuotojo kvalifikacijos kortelių išdavimas; Transporto priemonių nuosavybės teisės deklaravimas; Transporto priemonių registracijos mokesčio administravimas; Transporto priemonių registravimas, valstybinio registracijos numerio ženklų išdavimas; Registrų informacinių sistemų duomenų teikimas.

5.4. Suinteresuotų šalių reikalavimai AB „Regitra“ kyla iš:

5.4.1. tarptautinių teisės aktų;

5.4.2. Lietuvos Respublikos teisės aktų;

5.4.3. sutarčių ir susitarimų.

5.5. AB „Regitra“ užtikrina informacijos ir kibernetinį saugumą, prisiimdama įsipareigojimus ir atitikdama taikomus teisinius reikalavimus bei paskirstydama atsakomybes už informacijos ir kibernetinį saugumą.

5.6. Informacijos ir kibernetinio saugumo valdymas AB „Regitra“ yra pagrįstas rizikos valdymu. Informacijos saugumo rizikos vertinimas sudaro sąlygas, kad informacijos ir kibernetinio saugumo valdymo priemonės, taikomos AB „Regitra“ veikloje, atitiktų pagrindinius AB „Regitra“ veiklos bei informacijos ir kibernetinio saugumo tikslus.

5.7. AB „Regitra“ informacijos saugumo rizikų vertinamas atliekamas ne rečiau kaip kartą per metus arba įvykus reikšmingiems AB „Regitra“ pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui.

5.8. AB „Regitra“ ISVS vidaus auditas atliekamas kartu su atitikties vertinimu ne rečiau kaip kartą per metus arba įvykus reikšmingiems AB „Regitra“ pokyčiams, kurie gali turėti poveikį informacijos ir kibernetiniam saugumui. AB „Regitra“ atitikties vertinimą ne rečiau kaip kartą per 3 metus privalo atlikti nepriklausomi visuotinai pripažintų tarptautinių organizacijų sertifikuoti auditoriai Lietuvos Respublikos kibernetinio saugumo įstatymo nustatyta tvarka.

5.9. AB „Regitra“ turi būti vykdomas ISVS procesų ir kontrolės priemonių stebėjimas, matavimai, analizė ir įvertinimas.

5.10. AB „Regitra“ atliekama ISVS valdymo peržiūra atliekama ne rečiau kaip kartą per metus, siekiant įvertinti ISVS veiksmingumą ir efektyvumą bei nustatyti jo gerinimo sritis.

6. POLITIKOS ĮGYVENDINIMO PRIEMONĖS

6.1. Informacijos ir kibernetinio saugumo reikalavimų įgyvendinimas užtikrinamas ir valdomas nuosekliai planuojant, įgyvendinant, vertinant ir tobulinant informacijos saugumo valdymo sistemą, vadovaujantis ISO 27001 ir Lietuvos Respublikos teisės aktų reikalavimais. Su informacijos ir kibernetiniu saugumu susijusių aktualių teisės aktų sąrašas yra pateiktas vidiniame AB „Regitra“ dokumente „Informacijos saugumo valdymo sistemos vadovas“ – tai šios Politikos įgyvendinimą reglamentuojančių ISVS ir TIS tvarkų (tvarkos aprašų), planų, procedūrų bei numatytų kontrolės priemonių ir už jų įgyvendinimą atsakingų AB „Regitra“ padalinių ir darbuotojų bei suinteresuotųjų šalių atsakomybių ir funkcijų visuma, kuri detalizuota šiame dokumente (vadove) ir kituose AB „Regitra“ vidaus teisės aktuose, reglamentuojančiuose informacijos ir kibernetinio saugumo valdymą bei šios Politikos įgyvendinimą.

6.2. ISVS sudaro šios pagrindinės organizacinės ir techninės priemonės (bet neapsiribojant):

6.2.1. Prieigos teisių valdymas:

6.2.1.1. Informacinio ištekliaus savininko sprendimu prieigos teisės prie jo suteikiamos vadovaujantis principu „būtina žinoti“;

6.2.1.2. Užtikrinant tiekimo grandinės saugumą, suteikiant prieigas prie informacinio ištekliaus trečiosioms šalims, turi būti gaunamas jų patvirtinimas, kad prieigos bus naudojamos vadovaujantis šia Politika ir kitais informacijos ir kibernetinio saugumo reikalavimais, tik nurodytu tikslu, apimtimi ir būdais bei numatyta atsakomybė už nurodyto įsipareigojimo pažeidimą;

6.2.1.3. AB „Regitra“ sukurta, gauta ir naudojama informacija, nepriklausomai nuo jos formos ar laikmenos, klasifikuojama į viešąją ir konfidencialią informaciją. Prieigos teisės prie konfidencialios informacijos suteikiamos tik vadovaujantis principu „būtina žinoti“.

6.2.2. Duomenų perdavimo tinklų (toliau – Tinklų) sauga:

6.2.2.1. Tinklų saugumas užtikrinamas naudojant tam skirtas technines ir programines priemones ir vykdant nuolatinę jų veiklos stebėseną;

6.2.2.2. AB „Regitra“ Informacinius išteklius iš nuotolinės darbo vietos galima pasiekti tik šifruotu ryšiu.

6.2.3. Informacinių sistemų (toliau – IS) veiklos sauga:

6.2.3.1. AB „Regitra“ IS infrastruktūroje turi būti naudojamos kenkėjiškos programinės įrangos ir (ar) veiklos aptikimo, užkardymo ir stebėjimo priemonės;

6.2.3.2. Visų IS įrenginių saugos žurnaliniai įrašai, įskaitant operacines sistemas, duomenų bazes, taikomąsias programas turi būti kaupiami centralizuotai;

6.2.3.3. AB „Regitra“ privalo būti užtikrintas atsarginių kopijų kūrimas, saugojimas ir atkūrimo bandymų (testavimo) atlikimas.

6.2.4. TIS įrenginių sauga:

6.2.4.1. Įrenginiai turi atitikti AB „Regitra“ vidaus teisės aktuose nustatytus saugos reikalavimus.

6.2.5. Žmogiškasis faktorius:

6.2.5.1. Darbuotojai, valdymo organų nariai, paslaugų teikėjai ir (ar) kitos trečiosios šalys turi pareigą saugoti AB „Regitra“ informacinį turtą ir išteklius;

6.2.6. Kriptografija ir šifravimas:

6.2.6.1. AB „Regitra“ informacinių išteklių apsauga turi būti užtikrinama naudojant visuotinai pripažintas saugias šifravimo priemones, kurioms keliami reikalavimai nustatomi AB „Regitra“ vidaus teisės aktais;

6.2.6.2. Kriptografiniai raktai turi būti valdomi centralizuotai.

6.2.7. Fizinė sauga:

6.2.7.1. Fizinė prieiga prie AB „Regitra“ biurų ir kitų patalpų, kuriose saugomi AB „Regitra“ informaciniai ištekliai, turi būti ribojama ir kontroliuojama, taikant prevencines ir detekcines kontrolės priemones.

6.2.8. Pažeidžiamumų valdymas:

6.2.8.1. AB „Regitra“ periodiškai turi būti vykdomas informacinių išteklių ir IT komponentų pažeidžiamumų identifikavimas, vertinimas, stebėjimas ir šalinimas;

6.2.8.2. identifikuoti pažeidžiamumai turi būti klasifikuojami bei šalinami pagal prioritetus, atsižvelgiant į jų kritiškumo lygį.

6.2.9. TIS įsigijimas, kūrimas ir priežiūra:

6.2.9.1. naujai projektuojamos, kuriamos, įsigyjamos TIS bei esamų pokyčiai turi atitikti teisės aktuose nustatytus saugumo reikalavimus;

6.2.9.2. prieš pradedant naudoti TIS ar jų dalis, turi būti atliekamas saugos vertinimas. Draudžiama naudoti saugumo reikalavimų neatitinkančias informacines sistemas;

6.2.9.3. AB „Regitra“ naudojamos TIS ir jų komponentai (operacinės sistemos, duomenų bazių valdymo sistemos, kita susijusi programinė įranga) turi būti palaikomos gamintojo ir periodiškai atnaujinamos.

6.2.10. Tiekimo grandinės valdymas:

6.2.10.1. Trečiosios šalys, teikiančios TIS kūrimo bei priežiūros paslaugas, debesijos paslaugas AB „Regitra“ ar tvarkančios AB „Regitra“ informacinius išteklius, turi užtikrinti, kad jų infrastruktūra ir procesai atitinka jiems keliamus saugos reikalavimus;

6.2.10.2. turi būti užtikrintas trečiųjų šalių, teikiančių IT paslaugas, veiksmų stebėjimas ir registravimas.

6.2.11. Incidentų valdymas:

6.2.11.1. Darbuotojai, valdymo organų nariai, paslaugų teikėjai ir kitos trečiosios šalys turi pareigą pranešti apie pastebėtus informacijos saugumo ir kibernetinius incidentus (toliau – Incidentus);

6.2.11.2. Šių Incidentų valdymas turi apimti jo identifikavimą, vertinimą,

kategorizavimą ir prioritetizavimą, atsižvelgiant į Incidento poveikį, stabdymą bei šalinimą;

6.2.11.3. Patirtys, įgytos valdant Incidentus, turi būti pritaikomos, siekiant išvengti Incidentų ir (ar) ateityje sumažinti Incidentų pasireiškimo tikimybę ir poveikį.

6.2.12. Rizikų valdymas ir veiklos tęstinumo užtikrinimas:

6.2.12.1. Periodinis informacijos ir kibernetinio saugumo rizikų identifikavimas, vertinimas ir stebėsena atliekama vadovaujantis AB „Regitra“ rizikos valdymą reguliuojančiais teisės aktais;

6.2.12.2. Veiklos tęstinumas užtikrinamas vadovaujantis AB „Regitra“ veiklos tęstinumo užtikrinimą reglamentuojančiais teisės aktais.

6.3. Politikos įgyvendinimą ir konkrečias įgyvendinimo priemones, atsakomybes reglamentuojantys vidiniai teisės aktai apima informacijos ir kibernetinio saugumo rizikos analizę, atsakingų asmenų pareigas ir atsakomybes, informacijos saugumo ir kibernetinių incidentų valdymą, veiklos tęstinumą, TIS kopijavimą ir atstatymą, tiekimo grandinės saugumo užtikrinimą, TIS valdymą (įsigijimo, plėtojimo ir priežiūros saugumą, įskaitant spragų valdymą), ISVS veiksmingumo vertinimą, informacijos ir kibernetinio saugumo mokymus, kriptografijos ir šifravimo politiką ir procedūras, žmogiškųjų išteklių saugumą, fizinės prieigos ir IT turto valdymą, prieigų ir paskyrų valdymą.

7. BAIGIAMOSIOS NUOSTATOS

7.1. Politika įsigalioja ją patvirtinus.

7.2. Politika ir jos pakeitimai tvirtinami AB „Regitra“ valdybos sprendimu.

7.3. Su Politika supažindinami naujai priimami ir esami AB „Regitra“ darbuotojai. AB „Regitra“ užtikrina, kad su Politika būtų supažindintos trečiosios šalys, kurios AB „Regitra“ teikia prekes, paslaugas ar darbus, ir kurių teikimo metu suteikiama prieiga prie AB „Regitra“ tvarkomos ar valdomos informacijos ar informacinių išteklių.

7.4. Už Politikos parengimą, peržiūrą, kontrolę ir įgyvendinimą yra atsakingas AB „Regitra“ generalinis direktorius ar jo įgaliotas AB „Regitra“ padalinys ir (ar) darbuotojas.

7.5. Politika yra skelbiama viešai AB „Regitra“ interneto svetainėje.

7.6. Politika ir jos įgyvendinimą reglamentuojantys AB „Regitra“ generalinio direktoriaus patvirtinti vidaus teisės aktai yra peržiūrimi ne rečiau kaip kartą per metus ir atnaujinami pagal poreikį.

7.7. Bet koks Politikos ir kitų ISVS tvarkų reikalavimų pažeidimas laikomas informacijos ir kibernetinio saugumo valdymo pažeidimu, kuris gali daryti neigiamą įtaką AB „Regitra“ veiklos tęstinumui, pakenkti jos įvaizdžiui visuomenėje.

7.8. AB „Regitra“ darbuotojai ir trečiosios šalys, pažeidę šios Politikos ir ISVS tvarkų reikalavimus, atsako Lietuvos Respublikos teisės aktuose, AB „Regitra“ vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose nustatyta tvarka.

7.9. Politika taikoma tiek, kiek neprieštarauja Lietuvos Respublikos įstatymams ir (ar) kitiems galiojantiems teisės aktams.

_____