PATVIRTINTA
Akcinės bendrovės „Oro navigacija“
generalinio direktoriaus
2023 m. kovo 6 d.
įsakymu Nr. V-49

AKCINĖS BENDROVĖS „ORO NAVIGACIJA“ INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

TIKSLAS	Informacijos ir kibernetinio saugumo politika (toliau – Politika) apibrėžia akcinės bendrovės „Oro navigacija“ (toliau – Bendrovės) vadovybės poziciją ir atsakomybę informacijos ir kibernetinio saugumo srityje bei yra skirta pateikti vieningus saugumo valdymo principus bei užtikrinti efektyvų Bendrovės informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.
TAIKYMO SRITIS	Ši Politika privaloma Bendrovės valdybai, generaliniam direktoriui, visiems Bendrovės darbuotojams, praktikantams, visoms suinteresuotoms šalims ir kitiems Bendrovėje dirbantiems asmenims, įskaitant trečiųjų šalių darbuotojus. Politika taikoma kiekviename Bendrovės veiklos procese, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo.
PRIORITETAS	Informaciją laikome prioritetiniu mūsų veiklos ištekliu, todėl elektroninės, rašytinės, žodinės informacijos saugumas yra esminis siekis, norint užtikrinti Bendrovės patikimumą, finansinį stabilumą, veiklos tęstinumą ir suinteresuotų šalių reikalavimų vykdymą.

UŽTIKRINIMO KRYPTYS	Užtikrinti **saugią ir patikimą informacinę ir kibernetinę Bendrovės aplinką**, atsižvelgiant į Bendrovės strateginius tikslus ir neviršijant vadovybės valdomos ir prisiimamos rizikos lygio.
	Užtikrinti nuolatinį **informacijos saugumo valdymo ciklą,** vadovaujantis EN ISO/IEC 27001:2022 standarto reikalavimais ir kitų teisės aktų nustatytais reikalavimais bei keliant informacijos saugumo tikslus, atliekant rizikos vertinimą, vidaus auditą, siekiant identifikuoti neatitiktis ir gerinimo galimybes bei įgyvendinant atitiktį šią sritį reglamentuojantiems teisės aktams.
	Užtikrinti **Bendrovės veiklos tęstinumą**, t.y. elektroninių ryšių tinklų, informacinių sistemų, techninės ir programinės įrangos nepertraukiamą veiklą, informacijos saugumo ir kibernetinių incidentų valdymą ir savalaikį veiklos atstatymą.

PRINCIPAI	***Padidintas dėmesys informacijos ir kibernetinio saugumo kultūros vystymui ir palaikymui***. Darbuotojai turi tinkamai suvokti informacijos ir jos saugumo svarbą, galimą neigiamą poveikį Bendrovės veiklai, keliamų strateginių tikslų įgyvendinimui. Nuolatos didinamas visų Bendrovės darbuotojų atsparumas kibernetinėms grėsmėms periodiškai organizuojant mokymus, vykdant nuolatinę komunikaciją apie aktualias grėsmes ir priemones, leidžiančias išvengti incidentų.
	Rizikos vertinimas ir valdymas. Bendrovės svarbiausių veiklos procesų, informacijos ir kibernetinio saugumo grėsmių rizika vertinama periodiškai, taip pat atsiradus poreikiui (kuriant naujas ar keičiant esamas informacines sistemas ar veiklos procesus). Identifikuota rizika mažinama iki toleruojamo rizikos lygio taikant rizikos vertinimu pagrįstus, kainos ir efektyvumo atžvilgiu subalansuotas saugumo priemones.
	Atitiktis. Užtikrinti atitiktį teisės aktuose nustatytiems informacijos ir kibernetinio saugumo reikalavimams, Bendrovės sutartiniams įsipareigojimams su trečiosiomis šalimis, taikant rizikos vertinimu pagrįstas informacijos ir kibernetinio saugumo priemones.
	Sistemingas ir nuoseklus incidentų ir pažeidžiamumų valdymas. Valdant informacijos saugumo ir kibernetinius incidentus, užtikrinamas reikiamas reagavimas, suvaldymas ir mokymasis iš incidentų, siekiant išvengti jų pasikartojimo ar pažeidžiamumų išnaudojimo.

TAIKOMOS PRIEMONĖS	**Organizacinės priemonės.** Parengta ir puoselėjama informacijos saugumo vadybos sistema, atitinkanti ISO/IEC 27001:2022 tarptautinio standarto reikalavimus. Standarto pagrindu sukurtos procedūros, tvarkos kylančiai rizikai valdyti, vertinamos rizikos ir diegiamos reikiamos saugumo priemonės.
	Žmonių saugumo priemonės. Visų asmenų, siekiančių eiti pareigas Bendrovėje, praeitis ir asmens reputacija tikrinama. Darbuotojų kompetencijai keliami reikalavimai nustatyti darbuotojų pareigybių aprašymuose. Darbuotojų atsakomybės, įgaliojimai ir įsipareigojimai nustatyti procesų aprašuose, tvarkose bei instrukcijose.
	Fizinės saugumo priemonės apima patalpų (pvz., perimetro, įėjimo kontrolė, apsauga nuo išorinių grėsmių ir kt.) ir įrangos apsaugą nuo praradimo, sugadinimo ar vagystės. Bendrovė turi procedūras, skirtas neįprastiems veiksmams, kurie gali daryti poveikį Bendrovės fiziniam saugumui, nustatyti ir tinkamai reaguoti į tokius įvykius. Vykdoma nuolatinė stebėsena.
	Techninės priemonės: tinklo perimetro apsauga, techninės ir programinės įrangos saugus konfigūravimas, apsauga nuo kenksmingų priemonių, išorinio įsilaužimo prevencija, pažeidžiamumų vertinimas, elektroninio pašto ir naršyklės apsauga, audito žurnalų stebėjimas ir analizė, duomenų atkūrimo pajėgumas ir kt.
ĮSIPAREIGOJIMAI	Laikytis visų kibernetinio ir informacijos saugumo įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse ir prižiūrėti ir nuolat tobulinti informacijos saugumo valdymo sistemos efektyvumą.
	Skatinti ir propaguoti incidentų prevenciją užtikrinančias priemones bei vystyti Bendrovės darbuotojų informacijos saugumo kultūrą ir kibernetinę higieną (sąmoningumą).
	Užtikrinti efektyvų informacijos saugumo valdymo sistemos aprūpinimą reikiamais ištekliais, sudaryti sąlygas sąlygas Bendrovės darbuotojams tobulinti žinias informacijos ir kibernetinio saugumo bei asmens duomenų saugumo srityse.
ATSAKOMYBĖ	Bet koks Informacijos saugumo normų pažeidimas laikomas Informacijos saugumo incidentu, kuris gali daryti neigiamą įtaką Bendrovės veiklos tęstinumui, sugadinti ir pakenkti Bendrovės įvaizdžiui visuomenėje.
	Nedelsiant pranešti pastebėjus Bendrovės informacinių sistemų veiklos sutrikimą ar saugumo incidentą, kibernetinio saugumo spragą ar silpnąją vietą Bendrovės IT Pagalbos tarnybai el. paštu cirt@ans.lt arba telefonu +370 706 94707.
	Bendrovės darbuotojams ir trečiosioms šalims, pažeidusiems informacijos saugumo vadybos sistemos reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės.
POLITIKOS PERŽIŪRA IR SKLAIDA	Politika tvirtinama, keičiama ar naikinama Bendrovės generalinio direktoriaus įsakymu. Politiką rengia, reguliariai peržiūri ir atnaujina Bendrovės informacinės saugos įgaliotinis.
	Politika yra skelbiama viešai Bendrovės interneto svetainėje www.ans.lt ir prieinama visoms suinteresuotoms šalims.
	Šios Politikos nuostatos detalizuojamos ir įgyvendinamos priimant Bendrovės vidaus teisės aktus, derančius su Bendrovės strateginiais tikslais, teisiniais reikalavimais, tarptautiniais informacijos saugumo standartais ir gerosiomis praktikomis.