PATVIRTINTA
Akcinės bendrovės „Oro navigacija“
valdybos 2026 m. sausio 28 d.
posėdžio Nr. 2 sprendimu Nr. 6

AKCINĖS BENDROVĖS „ORO NAVIGACIJA“ INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITIKA

1. Tikslas	Įgyvendinti veiksmingą akcinės bendrovės „Oro navigacija“ informacijos saugumo, kibernetinio saugumo ir privatumo apsaugą, valdant rizikas, galinčias daryti poveikį aviacijos saugai, užtikrinant ankstyvą incidentų aptikimą ir reagavimą, didinant akcinės bendrovės „Oro navigacija“ atsparumą kibernetinėms grėsmėms ir palaikant saugią ir patikimą naudojamų tinklų ir informacinių sistemų veiklą. Kiti informacijos saugumo valdymo tikslai nustatomi akcinės bendrovės „Oro navigacija“ strateginiame veiklos plane ir vadovybės vertinamosios analizės metu.
2. Taikymo apimtis	Informacijos ir kibernetinio saugumo politika taikoma: ▪ visai akcinės bendrovės „Oro navigacija“ valdomai informacijai ir visam informaciniam turtui, nepriklausomai nuo jo formos ar gyvavimo ciklo etapo; ▪ visiems įrenginiams ir naudotojams, turintiems prieigą prie šių Bendrovės išteklių, tiek darbo vietoje, tiek už jo ribų, kai veikla susijusi su akcinės bendrovės „Oro navigacija“ funkcijomis ir sprendimais; ▪ visiems akcinės bendrovės „Oro navigacija“ informacijos išteklių naudotojams, įskaitant, bet neapsiribojant, akcinės bendrovės „Oro navigacija“ valdybos nariams, Audito komitetui, generaliniam direktoriui, akcinės bendrovės „Oro navigacija“ darbuotojams, Paslaugų teikėjams (tiekėjams) ir kitiems asmenims, kurie tvarko informaciją akcinės bendrovės „Oro navigacija“ vardu, atlikdami savo darbą ar vykdydami pareigas.
3. Politikos savininkas	Akcinės bendrovės „Oro navigacija“ Saugumo skyrius
4. Tvirtina	Akcinės bendrovės „Oro navigacija“ Valdyba
5. Politikos viešinimas	Informacijos ir kibernetinio saugumo politika skelbiama akcinės bendrovės „Oro navigacija“ dokumentų valdymo sistemoje ir išorinėje interneto svetainėje, pasiekiamoje adresu www.ans.lt, lietuvių ir anglų kalbomis.

I SKYRIUS
VARTOJAMI TERMINAI, APIBRĖŽTYS IR SANTRUMPOS

6.1. Audito komitetas	Patariamasis Valdybai kolegialus akcinės bendrovės „Oro navigacija“ organas.
6.2. BDAR	Bendrasis duomenų apsaugos reglamentas.
6.3. Bendrovė	Akcinė bendrovė „Oro navigacija“.
6.4. Bendrovės ISVS dalyvis	Bet kuris valdymo organas, akcinės bendrovės „Oro navigacija“ struktūrinis padalinys, darbuotojas ar kitas asmuo, įvardintas šios Politikos III skyriuje.
6.5. ES	Europos Sąjunga.
6.6. Generalinis direktorius	Akcinės bendrovės „Oro navigacija“ vienasmenis valdymo organas, jos vadovas, atsakingas už veiklos organizavimą.
6.7. Informaciniai ištekliai	Visi akcinės bendrovės „Oro navigacija“ turimi ar valdomi duomenys, informacija, informacinės sistemos, technologijos, dokumentai ir kiti su informacijos kūrimu, saugojimu, apdorojimu ar perdavimu susiję elementai, kurie yra būtini akcinės bendrovės „Oro navigacija“ veiklai ir tikslams pasiekti.

6.8. ISVS	Informacijos ir kibernetinio saugumo valdymo sistema
6.9. LR	Lietuvos Respublika
6.10. Paslaugų teikėjas (tiekėjas)	Fizinis ar juridinis asmuo, teikiantis akcinei bendrovei „Oro navigacija“ prekes, paslaugas ar darbus, kai vykdant sutartį (ar pavedimą) jam ir (ar) jo darbuotojams suteikiama prieiga prie Bendrovės informacijos, informacinio turto, riboto patekimo patalpų ir (ar) Bendrovės tinklų ir informacinių sistemų, arba kai teikiamos paslaugos yra susijusios su tinklais ir informacinėmis sistemomis ar kitu kritiniu informaciniu turtu.
6.11. Politika	Ši Informacijos ir kibernetinio saugumo politika.
6.12. Tinklų ir informacinė sistema (toliau – TIS)	Elektroninių ryšių tinklas, bet koks prietaisas arba tarpusavyje sujungtų arba susijusių prietaisų, iš kurių vienas ar daugiau pagal programą automatiškai apdoroja skaitmeninius duomenis, grupė arba skaitmeniniai duomenys, saugomi, tvarkomi, atkuriami arba perduodami nurodytomis priemonėmis jų valdymo, naudojimo, apsaugos ir priežiūros tikslais.
6.13. Valdyba	Kolegialus akcinės bendrovės „Oro navigacija“ valdymo organas

II SKYRIUS
TEISINIS PAGRINDIMAS

7. Politika parengta ir jos nuostatos taikomos vadovaujantis ES ir LR teisės aktų reikalavimais:	
7.1. ES 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/; ▪ 2017 m. kovo 1 d. Komisijos įgyvendinimo reglamentas (ES) 2017/373, kuriuo nustatomi oro eismo valdymo ir oro navigacijos paslaugų teikėjų, kitų oro eismo valdymo tinklo funkcijų vykdytojų ir tų subjektų priežiūros bendrieji reikalavimai, panaikinamas Reglamentas (EB) Nr. 482/2008, įgyvendinimo reglamentai (ES) Nr. 1034/2011, (ES) Nr. 1035/2011 ir (ES) 2016/1377 ir iš dalies keičiamas Reglamentas (ES) Nr. 677/2011; ▪ 2022 m. spalio 27 d. Komisijos įgyvendinimo reglamentas (ES) 2023/203, kuriuo nustatomos Europos Parlamento ir Tarybos reglamento (ES) 2018/1139 taikymo taisyklės, susijusios su Komisijos reglamentuose (ES) Nr. 1321/2014, (ES) Nr. 965/2012, (ES) Nr. 1178/2011, (ES) 2015/340, Komisijos įgyvendinimo reglamentuose (ES) 2017/373 ir (ES) 2021/664 nurodytoms organizacijoms ir Komisijos reglamentuose (ES) Nr. 748/2012, (ES) Nr. 1321/2014, (ES) Nr. 965/2012, (ES) Nr. 1178/2011, (ES) 2015/340, Komisijos įgyvendinimo reglamentuose (ES) 2017/373, (ES) Nr. 139/2014 ir (ES) 2021/664 nurodytoms kompetentingoms institucijoms taikytinais informacijos saugumo rizikos, galinčios turėti įtakos aviacijos saugai, valdymo reikalavimais, ir kuriuo iš dalies keičiami Komisijos reglamentai (ES) Nr. 1178/2011, (ES) Nr. 748/2012, (ES) Nr. 965/2012, (ES) Nr. 139/2014, (ES) Nr. 1321/2014, (ES) 2015/340 ir Komisijos įgyvendinimo reglamentai (ES) 2017/373 ir (ES) 2021/664; ▪ 2022 m. gruodžio 14 d. Europos Parlamento ir Tarybos direktyva (ES) 2022/2555 dėl priemonių aukštam bendram kibernetinio saugumo lygiui visoje Sąjungoje užtikrinti; ▪ 2023 m. liepos 14 d. Komisijos deleguotasis reglamentas (ES) 2023/1768, kuriuo nustatomos išsamios oro eismo valdymo ir (arba) oro navigacijos paslaugų sistemų ir sudedamųjų dalių sertifikavimo ir deklaravimo taisyklės;

	▪ 2023 m. rugsėjo 12 d. Komisijos įgyvendinimo reglamentas (ES) 2023/1769, kuriuo nustatomi oro eismo valdymo ir (arba) oro navigacijos paslaugų sistemų ir sudedamųjų dalių projektavimo arba gamybos veiklą vykdančių organizacijų patvirtinimo techniniai reikalavimai ir administracinės procedūros ir iš dalies keičiamas Įgyvendinimo reglamentas (ES) 2023/203; ▪ 2024 m. spalio 23 d. Europos Parlamento ir Tarybos reglamentas (ES) 2024/2847 dėl horizontaliųjų kibernetinio saugumo reikalavimų, keliamų produktams su skaitmeniniais elementais, kuriuo iš dalies keičiami reglamentai (ES) Nr. 168/2013 bei (ES) 2019/1020 ir Direktyva (ES) 2020/1828 (Kibernetinio atsparumo aktas).
7.2. LR teisės aktai	▪ Lietuvos Respublikos kibernetinio saugumo įstatymas; ▪ Kibernetinio saugumo reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo reikalavimų įgyvendinimo“; ▪ Lietuvos Respublikos komercinių paslapčių teisinės apsaugos įstatymas; ▪ Lietuvos Respublikos darbo kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas; ▪ Lietuvos Respublikos viešųjų pirkimų įstatymas; ▪ Lietuvos Respublikos civilinio kodekso patvirtinimo, įsigaliojimo ir įgyvendinimo įstatymas; ▪ Kiti LR teisės aktai, reglamentuojantys informacijos ir kibernetinį saugumą, taip pat asmens duomenų apsaugą.
8. Taikant Politiką taip pat vadovaujamasi tarptautiniais standartais ir (ar) gerosiomis praktikomis, tarp jų:	
8.1. Gerosios praktikos	▪ Lietuvos standartas LST EN ISO/IEC 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai (ISO/IEC 27001:2022)“; ▪ Lietuvos standartas LST EN ISO/IEC 27002:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo kontrolės priemonės (ISO/IEC 27002:2022)[1]“.
8.2. Susiję dokumentai	Šios Politikos nuostatos detalizuojamos ir įgyvendinamos priimant Bendrovės vidaus teisės aktus, derančius su Bendrovės strateginiais tikslais, teisiniais reikalavimais, tarptautiniais standartais ir gerosiomis praktikomis. Bendrovės vidaus teisės aktai privalo neprieštarauti šiai Politikai.
9. Jei yra teisės aktų ir Politikos neatitikimų, Politika taikoma tiek, kiek neprieštarauja teisės aktams.	
10. Politikoje vartojamos sąvokos suprantamos taip, kaip jos vartojamos aukščiau apibrėžtuose teisės aktuose.	

III SKYRIUS
INFORMACIJOS SAUGUMO VADYBOS SISTEMOS DALYVIAI IR JŲ PAREIGOS

11. Visi Bendrovės ISVS dalyviai turi pareigą laikytis šios Politikos, teisės aktuose įtvirtintų informacijos ir kibernetinio saugumo reikalavimų bei ikisutartinių ir (ar) sutartinių įsipareigojimų.	
12. Bendrovės ISVS dalyvauja ir turi atitinkamas funkcijas ir pareigas:	
12.1. Bendrovės valdyba	▪ Tvirtinti šią Politiką; ▪ Nustatyti Bendrovės informacijos ir kibernetinio saugumo užtikrinimo kryptis, tikslus, siekius ir principus.

[1] Standartas yra perimtas iš Europos standarto EN ISO/IEC 27002:2022 „Information security, cybersecurity and privacy protection – Information security controls“.

12.2. Generalinis direktorius	▪ Užtikrinti Politikos įgyvendinimą, vadovaudamas šiam procesui, prisiimdamas įsipareigojimus[2] bei paskirstydamas atsakomybę už informacijos ir kibernetinį saugumą; ▪ Užtikrinti, kad informacijos ir kibernetinio saugumo rizikų klausimai būtų neatsiejama Bendrovės strateginių sprendimų ir veiklos procesų dalimi; ▪ Skirti reikiamus išteklius, reikalingus ISVS užtikrinimui ir identifikuotų rizikų valdymui, įskaitant žmogiškuosius, finansinius išteklius, procesus, įrankius ir technologijas.
12.3. Kibernetinio saugumo vadovas	▪ Užtikrinti, kad Politika ir informacijos ir kibernetinio saugumo įgyvendinimą reglamentuojantys dokumentai būtų parengti ir periodiškai atnaujinami; ▪ Organizuoti Bendrovės atitikties informacijos ir kibernetinio saugumo reglamentuojantiems teisės aktams bei informacijos saugumo rizikos vertinimus; ▪ Organizuoti Bendrovės darbuotojų mokymus informacijos ir kibernetinio saugumo klausimais; ▪ Koordinuoti TIS kibernetinių incidentų tyrimus, užtikrinti bendradarbiavimą su kompetentingomis institucijomis ir inicijuoti neatitikčių šalinimo veiksmus. ▪ Teikti TIS administratoriui, saugos įgaliotiniui ir (ar) naudotojams privalomus vykdyti nurodymus ir pavedimus, susijusius su Politikos ir informacijos ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatytų reikalavimų įgyvendinimu.
12.4. Saugos įgaliotinis	▪ Užtikrinti, kad Politikos ir informacijos ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose nustatyti reikalavimai būtų įgyvendinami priskirtuose TIS, vykdyti kibernetinio saugumo reikalavimų įgyvendinimo priežiūrą ir teikti nurodymus TIS administratoriams ir kitiems atsakingiems asmenims siekiant laiku identifikuoti ir pašalinti saugumo spragas; ▪ Vykdyti Bendrovės atitikties informacijos ir kibernetinio saugumo reglamentuojantiems teisės aktams bei informacijos saugumo rizikos vertinimo procesų įgyvendinimą; ▪ Organizuoti ir vykdyti kibernetinio saugumo priemonių diegimą ir stebėseną, rengti informaciją apie incidentus, dalyvauti jų tyrimuose ir teikti duomenis kibernetinio saugumo vadovui; ▪ Koordinuoti Bendrovės darbuotojų mokymus, kibernetinio saugumo temomis ir užtikrinti jų informuotumą apie grėsmes, rizikas ir prevencines priemones.
12.5. Asmens duomenų apsaugos pareigūnas	▪ Prižiūrėti, kaip laikomasi BDAR, kitų ES ir nacionalinių duomenų apsaugos nuostatų ir Bendrovės politikos asmens duomenų apsaugos srityje; ▪ Konsultuoti dėl poveikio asmens duomenų apsaugai vertinimo ir stebi jo įgyvendinimą; ▪ Atsakyti į duomenų subjektų užklausas dėl jų teisių pagal BDAR ir kitus asmens duomenų apsaugą reglamentuojančius teisės aktus; ▪ Bendradarbiauti su Valstybine duomenų apsaugos inspekcija ar kitomis priežiūros institucijomis asmens duomenų klausimais.
12.6. TIS savininkas	▪ Planuoti TIS veiklas ir teikti privalomus nurodymus TIS administratoriui; ▪ Užtikrinti tinkamą TIS veikimą ir saugumą bei skatinti jų našumą; ▪ Užtikrinti tinkamą TIS problemų valdymą;

[2] Bendrovės vadovybės įsipareigojimai numatyti Akcinės bendrovės „Oro navigacija“ saugos, kokybės, saugumo ir atitikties politikoje.

	▪ Planuoti, vykdyti ir prižiūrėti TIS projektus; ▪ Ieškoti ir diegti naujus TIS sprendimus efektyvumui didinti; ▪ Atlikti kitas Politikoje ir informacijos ir kibernetinio saugumo įgyvendinimą reglamentuojančiuose dokumentuose bei kituose teisės aktuose, reglamentuojančiuose kibernetinį saugumą, nustatytas ir TIS savininkui priskirtas funkcijas.
12.7. TIS administratorius	▪ Valdyti TIS naudotojų prieigos teises; ▪ Prižiūrėti TIS komponentus (kompiuterių, operacinių sistemų, duomenų bazių, taikomųjų programų, saugasienių, įsibrovimo aptikimo sistemų); ▪ Valdyti TIS komponentų sąranką; ▪ Nustatyti TIS pažeidžiamas vietas; ▪ Nustatyti ir stebėti saugumo reikalavimų atitiktį, reagavimą į kibernetinius incidentus.
12.8. Saugumo operacijų centras	▪ Nuolat stebėti Bendrovės TIS veiklą, kibernetinio saugumo įvykius, juos apdoroti ir laiku eskaluoti; ▪ Atlikti su kibernetinių incidentų valdymu susijusius veiksmus (aptikimą, užkardymą); ▪ Rinkti informaciją apie pažeidžiamumus, vykdo jų analizę, koordinuoja pažeidžiamumų valdymo sprendimų veiksmus su paveiktais subjektais; ▪ Analizuoti kibernetines grėsmes ir į jas reaguoti; ▪ Teikti kibernetinio saugumo rekomendacijas Bendrovės darbuotojams.
12.9. Veiklos tęstinumo valdymo grupė	▪ Koordinuoti Bendrovės veiklos tęstinumo planų rengimą ir atnaujinimą; ▪ Vertinti Bendrovės veiklos tęstinumo rizikas ir nustatyti kritines funkcijas; ▪ Organizuoti Bendrovės veiklos tęstinumo priemonių testavimą ir mokymus.
12.10. Veiklos atkūrimo grupė	▪ Organizuoti Bendrovės paslaugų, duomenų ir infrastruktūros atkūrimą; ▪ Įgyvendinti atkūrimo veiksmus pagal nustatytus prioritetus; ▪ Koordinuoti techninius atkūrimo veiksmus su Bendrovės struktūriniais padaliniais ir paslaugų teikėjais (tiekėjais); ▪ Analizuoti atkūrimo procesą ir teikti rekomendacijas tobulinimui.
12.11. Darbuotojai	▪ Kasdienėje veikloje, vykdant darbo funkcijas ir priimant sprendimus, privalo laikytis informacijos ir kibernetinio saugumo reikalavimų ir užtikrinti saugų jiems patikėtos arba jiems žinomos informacijos ir informacinio turto naudojimą; ▪ Saugoti konfidencialią informaciją ir neskelbti jos tretiesiems asmenims be nustatyto leidimo; ▪ Identifikuoti, vertinti ir stebėti informacijos ir kibernetinio saugumo rizikas, parinkti ir taikyti priemones joms suvaldyti, vadovaujantis nustatytais reikalavimais.
12.12. Paslaugų teikėjai (tiekėjai)	▪ Laikytis Politikos, ES ir LT teisės aktuose bei sutartyse nustatytų informacijos ir kibernetinio saugumo reikalavimų; ▪ Įsipareigoja saugoti konfidencialią informaciją taikant tinkamas apsaugos priemones ir neskelbti, neatskleisti jos tretiesiems asmenims be Bendrovės leidimo, jeigu Lietuvos Respublikos įstatymai bei kiti teisės aktai nenustato kitaip; ▪ Užtikrinti, kad jų infrastruktūra ir procesai atitiktų jiems keliamus informacijos ir kibernetinio saugumo reikalavimus; ▪ Atsako už saugų jiems patikėto Bendrovės informacinio turto naudojimą; ▪ Užtikrina, kad imsis pakankamų priemonių rizikoms, susijusioms su subrangovais, jų atliekamais darbais ir tiekimo grandine, suvaldyti.
13. Bendrovė bendradarbiauja su Lietuvos Respublikos institucijomis ir tarptautinėmis organizacijomis, formuojančiomis ir įgyvendinančiomis kibernetinio saugumo politiką, dalyvauja profesiniuose forumuose ir	

iniciatyvose, dalijasi informacija apie informacijos ir kibernetinio saugumo grėsmes bei gerąja saugumo praktika, siekdama stiprinti bendrą saugumo atsparumą.

IV SKYRIUS
BENDROVĖS INFORMACIJOS IR KIBERNETINIO SAUGUMO UŽTIKRINIMO PRINCIPAI IR ĮSIPAREIGOJIMAI

14. Siekdama Politikos tikslų, Bendrovė įsipareigoja laikytis bendrųjų teisės principų, informacijos ir kibernetinio saugumo reikalavimų, diegti ir nuolat gerinti ISVS, vadovaujantis tarptautiniu standartu ISO/IEC 27001, taikydama inovatyvius, rizikai proporcingus organizacinius, žmogiškuosius, fizinius ir technologinius saugumo kontrolės sprendimus.

15. Bendrovė, siekdama užtikrinti informacinių išteklių apsaugą ir veiksmingą rizikos valdymą, įsipareigoja vadovautis šiais pagrindiniais informacijos saugumo principais:

Pagrindiniai principai:		**15.1. VALDYMAS: Užtikrinti nuoseklų, rizika grįstą ir brandų informacijos saugumo valdymą, stiprinant Bendrovės ISVS dalyvių sąmoningumą ir atsakomybę už saugumą.**		**15.2. IDENTIFIKAVIMAS: Užtikrinti, kad visi informaciniai ištekliai būtų identifikuoti, įvertinti ir valdomi remiantis rizika, siekiant tinkamai apsaugoti informaciją visame jos gyvavimo cikle.**
		**15.3. APSAUGA: Užtikrinti informacijos apsaugą taikant rizika grįstas ir teisės aktų reikalavimus atitinkančias kontrolės priemones.**		**15.4. APTIKIMAS, REAGAVIMAS, ATKŪRIMAS: Užtikrinti savalaikį saugumo įvykių aptikimą, veiksmingą reagavimą ir incidentų šalinimą, atkuriant veiklą bei mažinant galimą poveikį Bendrovei.**

16. Pagrindiniai Bendrovės informacijos ir kibernetinio saugumo principai užtikrinami šiomis kryptimis:

16.1. Valdymo principas	16.1.1. Paskirstyta atsakomybė ir atitinkamos pareigos ISVS dalyviams. 16.1.2. Informacijos ištekliai tvarkomi laikantis visų Bendrovei taikomų įstatymų ir kitų susijusių teisės aktų reikalavimų. 16.1.3. Saugumo rizikos valdymo veikla yra integruota į Bendrovės rizikos valdymo sistemą. Taikomas holistinis požiūris į rizikos valdymą. 16.1.4. Saugumo rizika yra priimama prieš jas leidžiant naudoti ir valdoma viso gyvavimo ciklo metu.
16.2. Identifikavimo principas	16.2.1. Visas Bendrovės informacinis turtas aiškiai identifikuotas, t.y. tinkamai inventorizuojamas ir prižiūrimas, bei paskirti už jį atsakingi savininkai. Nustatoma turto vertė ir kritiškumas veiklai. 16.2.2. Nustatyti ir dokumentuoti informacinių išteklių konfidencialumo, vientisumo, autentiškumo ir prieinamumo reikalavimai. 16.2.3. Informacija Bendrovėje skirstoma į viešą, viešai neteiktiną ir neskelbtiną, konfidencialią ir ypatingos svarbos, atitinkamai žymima naudojant Šviesoforo metodą[3]. 16.2.4. Informacijos saugumo klasifikacija ir jos apsaugos lygiai nustatomi proporcingai turto svarbai. 16.2.5. ISVS yra pagrįsta rizikų identifikavimu, vertinimu ir stebėsena. Rizikos vertinimas atliekamas bent kartą per metus arba atsiradus pokyčiams, siekiant nustatyti ir įvertinti įvairias informacijos saugumo rizikas ir nustatyti reikiamų kontrolės priemonių prioritetus, atsižvelgiant į poveikį veiklai ir rizikos atsiradimo tikimybę. Rizikos vertinimo rezultatai ir susiję sprendimai dokumentuojami.

[3] Daugiau informacijos apie Šviesoforo metodą oficialiame puslapyje: https://www.first.org/tlp/.

	16.2.6. Įgyvendinamos rizikos mažinimo priemonės, pagrįstos vertinimų rezultatais. Identifikuota rizika mažinama iki toleruojamo rizikos lygio taikant rizikos vertinimu pagrįstas saugumo priemones.
16.3. Apsaugos principas	**16.3.1. Fizinis ir aplinkos saugumo valdymas:** 16.3.1.1. Bendrovėje įrengti tinkami fizinio saugumo perimetrai ir įėjimo kontrolė, siekiant užkirsti kelią neteisėtai fizinei prieigai. 16.3.1.2. Fizinė prieiga į Bendrovės teritoriją, prie TIS, infrastruktūros ir įrenginių suteikiama tik įgaliotiems Bendrovės darbuotojams. 16.3.1.3. Bendrovės teritorijoje draudžiama filmuoti ar fotografuoti negavus atsakingų asmenų leidimo. 16.3.1.4. Draudžiama į Bendrovės teritoriją įvežti/įnešti šiuos daiktus: ginklus, jų priedėlius ir šaudmenis ar jų imitacijas, sprogstamuosius įtaisus ir sprogiąsias medžiagas ar jų imitacijas, narkotikus ir narkotines medžiagas bei alkoholinius gėrimus, kitus, atvirą liepsną naudojančius ar kibirkštį skleidžiančius/sukeliančius, pavojingus daiktus, išskyrus tiesioginiam darbui, kuriam turi būti išduotas leidimas, naudojamus įrankius ar prietaisus. **16.3.2. Žmogiškųjų išteklių valdymas:** 16.3.2.1. Visi kandidatai prieš pradedant dirbti Bendrovėje patikrinami. Bendrovės darbuotojai tikrinami periodiškai. Kandidatų, darbuotojų ir dirbančių Bendrovei Paslaugų teikėjų (tiekėjų) patikrinimai vykdomi vadovaujantis Lietuvos Respublikos aviacijos įstatymu ir Lietuvos Respublikos nacionaliniam saugumui užtikrinti svarbių objektų apsaugos įstatymu. 16.3.2.2. Paslaugų teikėjų (tiekėjų) darbuotojai ar trečioji šalis, su kuria susiję Paslaugų teikėjo (tiekėjo) darbuotojai, gali būti įpareigoti (-a) pateikti leidimus dirbti su atitinkamos kategorijos informacija. 16.3.2.3. Paslaugų teikėjų (tiekėjų) darbuotojai ir jiems dirbantys asmenys privalo turėti reikalingus įgūdžius ir (ar) kvalifikaciją ir pateikti tai atitinkantį įrodymą, leidžiantį dirbti su konkrečiu Bendrovės informaciniu ištekliumi, kai tai yra būtina arba reikalaujama. **16.3.3. Saugumo mokymasis ir sąmoningumo didinimas:** 16.3.3.1. Bendrovė rūpinasi darbuotojų kibernetinės higienos praktika – visi darbuotojai ir Paslaugų teikėjų (tiekėjų), kuriems suteikiama prieiga prie Bendrovės informacijos ar informacinio turto, privalo būti tinkamai apmokyti informacijos ir kibernetinio saugumo klausimais. 16.3.3.2. Naujai priimti Bendrovės darbuotojai darbo pradžioje privalo išklausyti ir baigti įvadinius mokymus, kuriuose nagrinėjamos ir informacijos ir kibernetinio saugumo temos. 16.3.3.3. Visi Bendrovės darbuotojai, taip pat Paslaugų teikėjų (tiekėjų) darbuotojai, kuriems suteikta prieiga prie Bendrovės informacijos ar informacinio turto, privalo periodiškai dalyvauti mokymuose, kuriuose suteikiamos saugios veiklos kibernetinėje erdvėje žinios, o saugumo sąmoningumo lygis nuosekliai keliamas (Bendrovės mokymuose arba pateikiant lygiaverčių mokymų įrodymus). **16.3.4. Prieigos valdymas:** 16.3.4.1. Prieiga prie Bendrovės informacinio turto suteikiama tik Bendrovės įgaliotiems naudotojams. Prieiga reguliariai peržiūrima. 16.3.4.2. Prieiga prie Bendrovės informacinio turto suteikiama informacinio turto savininko sprendimu, vadovaujantis mažiausios privilegijos ir „būtina žinoti“ principais, tik darbo funkcijoms ar pareigoms atlikti. 16.3.4.3. Prieigai prie Bendrovės informacinio turto naudojamas patikimas ir saugus tapatybės bei prieigos valdymas. Kiekvienas sistemų naudotojas turi būti unikaliai atpažįstamas.

16.3.4.4. Darbuotojams prisijungti prie Bendrovės elektroninio pašto ir TIS leidžiama tik iš Bendrovės išduotų įrenginių.
16.3.4.5. Suteikiant prieigas prie Bendrovės informacinio turto trečiosioms šalims, turi būti gaunamas trečiųjų šalių 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.
16.3.4.6. Paslaugų teikėjams (tiekėjams) suteikiama nuotolinė prieiga prie Bendrovės informacinių išteklių šifruojama taikant virtualaus privataus tinklo (VPN) technologiją ir sesijoje dalyvaujant Bendrovės darbuotojams. Bet kokia nesankcionuota nuotolinė prieiga prie Bendrovės informacinio turto draudžiama.

16.3.5. Informacinių sistemų įsigijimas, kūrimas ir priežiūra:

16.3.5.1. TIS yra projektuojamos, diegiamos, prižiūrimos, vystomos ir likviduojamos atsižvelgiant į jų kritiškumą Bendrovės veiklai ir konfidencialumo, vientisumo, autentiškumo bei prieinamumo reikalavimus.
16.3.5.2. TIS, juos sudarančius komponentus tiekia ir palaiko tik patikimi Paslaugų teikėjai (tiekėjai). Draudžiama naudoti nepatikimų gamintojų įrangą, technologijas ar kitas susijusias paslaugas ar prekes.
16.3.5.3. Paslaugų teikėjų (tiekėjų) siūlomos prekės (įskaitant jų sudedamąsias dalis bei prekių ir jų dalių gamintojus), paslaugos ir darbai turi nekelti grėsmės nacionaliniam saugumui ir atitikti taikomus tarptautinių ir nacionalinių sankcijų reikalavimus. Paslaugų teikėjai (tiekėjai) negali turėti verslo ryšių su subjektais, keliančiais grėsmę nacionaliniam saugumui[4].
16.3.5.4. TIS projektuojamos ir konfigūruojamos pagal saugų projektavimo principą *(angl. secure by design)*, atsižvelgiant į saugumo riziką ir visus susijusius informacijos saugumo kontrolės priemonių reikalavimus.
16.3.5.5. Saugus programinės ar techninės įrangos kūrimo procesas turi būti užtikrinamas visuose etapuose: reikalavimų apibrėžimuose, dizaino kūrime, diegime, patvirtinime, išleidime, mokymuose ir priežiūroje.
16.3.5.6. Bet kokia nauja diegiama technologija Bendrovėje turi būti patvirtinta atsakingų Bendrovės darbuotojų, o ją naudoti galima tik gavus jų leidimą. Taip pat privaloma užtikrinti, kad technologijos atitiktų aviacijos saugos ir saugumo reikalavimus.
16.3.5.7. Produktuose neturi būti jokių paslėptų savybių, galinčių silpninti saugumą, įskaitant kenkėjišką programinę įrangą, neteisėtą prieigą ar funkcijas bei kitus saugumo pažeidimus. Į Bendrovės infrastruktūrą gali būti diegiamos tik patikimos ir palaikomos TIS.
16.3.5.8. Bendrovės TIS naudojama trečiųjų šalių programinė įranga turi atitikti saugumo reikalavimus ir būti licencijuota.
16.3.5.9. Prieš diegiant TIS į operacinę aplinką ir reguliariai jų veikimo metu atliekami pažeidžiamumų vertinimai, o aptikti pažeidžiamumai nedelsiant šalinami.
16.3.5.10. Bendrovės veiklai kritinėms TIS periodiškai atliekami įsiskverbimo testavimai, kurie koordinuojami įgaliotų Bendrovės darbuotojų.
16.3.5.11. Draudžiama savavališkai skanuoti Bendrovės TIS, ieškant pažeidžiamumų ar stebint duomenų srautą. Tokios priemonės gali būti taikomos tik tada, kai jos būtinos tiesioginėms pareigoms atlikti ir suderintos su Bendrovės darbuotoju, atsakingu už informacijos ir kibernetinį saugumą.

16.3.6. Informacinių sistemų veiklos saugumas:

16.3.6.1. Kompiuterinėse darbo vietose turi būti naudojamos kenkėjiškos programinės įrangos ir (ar) veiklos aptikimo, užkardymo ir stebėjimo priemonės.

[4] Lietuvos Respublikos Vyriausybės 2022-03-29 nutarimas Nr. 22-4687 „Dėl Lietuvos Respublikos viešųjų pirkimų įstatymo 92 straipsnio 13, 14 ir 15 dalių nuostatų įgyvendinimo".

	16.3.6.2. Visų Bendrovės TIS, tinklo įrenginių ir kitų įrenginių žurnaliniai įrašai, įskaitant operacinės sistemos, duomenų bazių, taikomųjų programų, turi būti kaupiami centralizuotai. **16.3.7. Duomenų saugumas:** 16.3.7.1. Duomenys šifruojami tiek juos saugant, tiek perduodant tarp skirtingų Bendrovės naudojamų TIS. 16.3.7.2. Darbuotojai bet kokiai korespondencijai, kurioje yra Bendrovės duomenų, arba kuri su jais susijusi, naudoja tik Bendrovės el. pašto adresus (ne asmenines el. pašto ar komunikacijos platformos paskyras). 16.3.7.3. Komunikacija, kurios turinį sudaro konfidenciali informacija, įskaitant asmens duomenis, turi būti vykdoma tik saugiu ryšio kanalu, naudojantis saugaus elektroninio pašto žinučių ir dokumentų apsikeitimo sprendimu https://cloud.ans.lt/. 16.3.7.4. Bendrovėje palaikoma „švaraus stalo“ ir „švaraus ekrano“ politika, draudžianti palikti dokumentus, bylas, informacijos laikmenas, įrenginius, kuriuose yra saugomos informacijos, be priežiūros ir papildomos apsaugos. 16.3.7.5. Reguliariai kuriamos ir saugiai testuojamos duomenų atsarginės kopijos.
16.4. Aptikimo principas	16.4.1. Įvykių žurnalai privalo būti renkami ir analizuojami realiu laiku, o aptikti saugumo įvykiai nedelsiant identifikuojami ir valdomi pagal Bendrovėje nustatytas incidentų valdymo procedūras. 16.4.2. Apie saugumo incidentus tiek Bendrovės viduje, tiek išorėje atitinkamoms įstaigoms ir suinteresuotosioms šalims pranešama nustatytais terminais.
16.5. Reagavimo ir atkūrimo principai	16.5.1. Įvykiai, kurie perauga į incidentus, valdomi pagal incidentų valdymo procedūras. 16.5.2. Reagavimo į incidentus, veiklos tęstinumo ir atkūrimo po nelaimių planai parengti ir prireikus įgyvendinami siekiant atkurti įprastą veiklą saugumo incidentų metu ir po jų ir sumažinti poveikį veiklos tęstinumui. 16.5.3. Po kiekvieno incidento atliekama analizė ir peržiūra, siekiant patobulinti reagavimo ir atkūrimo procesus.

V SKYRIUS
ATITIKTIS

17. Bendrovė, vykdydama veiklą, siekia atitikti jos veiklą reglamentuojančių teisės aktų, sutartinių įsipareigojimų reikalavimus bei užtikrina atitiktį šiai Politikai. Vykdomi atitikties Politikai ir susijusiems teisės aktų reikalavimams veiksmingumo vertinimai, vidaus ir išorės auditai, vadovybės peržiūros, vertinami Bendrovės darbuotojų ir suinteresuotųjų šalių atsiliepimai. Nustatomi ir įgyvendinami taisomieji ir gerinimo veiksmai.

18. Bendrovė turi teisę atlikti informacijos ir kibernetinio saugumo vertinimą ar kitus informacijos ir kibernetinio saugumo patikrinimo veiksmus, susijusius su Bendrovės informacinių išteklių kūrimu, vystymu, diegimu ir (ar) naudojimu, siekiant įsitikinti, ar laikomasi teisinių reikalavimų ir šios Politikos nuostatų.

19. Bet koks informacijos ir kibernetinio saugumo reikalavimų nesilaikymas ar galimi ir tikėtini nukrypimai turi būti dokumentuoti, įskaitant privalomą rizikos vertinimą ir sutartas kontrolės priemones. Politikos ir susijusių teisės aktų nuostatų taikymo išimtis tvirtina Bendrovės generalinis direktorius, užtikrinant jų atsekamumą.

VI SKYRIUS
ATSAKOMYBĖ

20. Bet koks informacijos ar kibernetinio saugumo normų pažeidimas laikomas informacijos saugumo įvykiu, galinčiu sutrikdyti Bendrovės veiklos tęstinumą, sukelti finansinius nuostolius, pakenkti Bendrovės reputacijai, sumažinti klientų ir partnerių pasitikėjimą bei lemti teisines bei reguliacines pasekmes.

21. Pareiga pranešti apie informacijos ir kibernetinio saugumo grėsmę, incidentą ar reikalavimų pažeidimą taikoma Bendrovės Valdybos, Audito komiteto nariams, generaliniam direktoriui, visiems Bendrovės darbuotojams ir Paslaugų teikėjams (tiekėjams).
Pastebėjus Bendrovės TIS veiklos sutrikimą, saugumo pažeidimą, kibernetinio saugumo spragą ar silpnąją vietą, privaloma nedelsiant informuoti Bendrovės Informacinių technologijų skyrių:
✉ el. p. **cirt@ans.lt** arba
☎ tel. **+370 706 94707**.

22. Bendrovės darbuotojams ir Paslaugų teikėjams (tiekėjams), pažeidusiems šią Politiką ir Bendrovėje taikomus ISVS reikalavimus, gali būti taikomos Lietuvos Respublikos įstatymuose, Bendrovės vidaus teisės aktuose, sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės.

VII SKYRIUS
BAIGIAMOSIOS NUOSTATOS

23. Su šia Politika supažindinami Bendrovės Valdybos, Audito komiteto nariai, generalinis direktorius, visi esami ir naujai priimami Bendrovės darbuotojai, Paslaugų teikėjai (tiekėjai) bei kitos trečiosios šalys, vykdančios sutartinius įsipareigojimus.

24. Politika peržiūrima periodiškai, bet ne rečiau kaip kartą per metus, arba įvykus esminiams Bendrovės veiklos ir reguliacinės aplinkos pokyčiams, turintiems įtakos ISVS įgyvendinimui, ir esant poreikiui atnaujinama.

25. Politika tvirtinama ir keičiama Bendrovės Valdybos posėdžio protokoliniu sprendimu.

_____