Akcinė bendrovė
Klaipėdos valstybinio jūrų uosto direkcija

KVJUD
REGISTRUOTA
2026-10-07 Nr. KT-2026-12

PATVIRTINTA
Akcinės bendrovės Klaipėdos valstybinio jūrų uosto direkcijos stebėtojų tarybos
2024 m. rugsėjo mėn. 19 d. sprendimu
(2024 m. rugsėjo mėn.25 d. posėdžio protokolo Nr. STP-13)
Nauja redakcija patvirtinta 2026 m. rugpjūčio 21 d. sprendimu
(2026 m. rugsėjo 4 d. posėdžio protokolo Nr. STP-11/2026)

AKCINĖS BENDROVĖS KLAIPĖDOS VALSTYBINIO JŪRŲ UOSTO DIREKCIJOS INFORMACIJOS SAUGOS POLITIKA

Tikslas:

1. Nustatyti akcinės bendrovės Klaipėdos valstybinio jūrų uosto direkcijos (toliau – įmonė arba Uosto direkcija) informacijos ir kibernetinio saugumo užtikrinimo kryptis ir principus, siekiant suvaldyti informacijos saugos grėsmių rizikas iki toleruojamo lygio.

2. Informacijos saugos politika (toliau – Politika) apibrėžia įmonės vadovaujančių darbuotojų poziciją ir atsakomybę informacijos ir kibernetinio saugumo srityje. Ji yra skirta pateikti vieningus saugumo valdymo principus bei užtikrinti efektyvų įmonės informacijos saugumo valdymo proceso įgyvendinimą.

Taikymo sritis:

Politika taikoma visiems įmonės darbuotojams, įskaitant trečiąsias šalis. Politika taikoma kiekvienoje įmonės lokacijoje, veikloje ir procese, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo.

1. Bendroji dalis

Informacijos vaidmuo įmonės veikloje yra ypač svarbus. Elektroninės, rašytinės, žodinės informacijos saugumas yra esminis siekis, norint užtikrinti įmonės patikimumą, finansinį stabilumą, veiklos tęstinumą ir suinteresuotų šalių reikalavimų vykdymą.

2. Informacijos saugos užtikrinimo kryptys ir principai

2.1.**Mokymai ir švietimas**. Įmonėje turi būti vystoma informacijos saugos kultūra, kad darbuotojai tinkamai suvoktų informacijos ir jos saugos svarbą, galimą neigiamą poveikį įmonės veiklai, jiems keliamų tikslų įgyvendinimui. Turi būti nuolatos didinamas visų darbuotojų atsparumas informacijos saugos grėsmėms periodiškai organizuojant mokymus, tikrinant darbuotojų žinias, vykdant nuolatinę komunikaciją apie įmonei aktualias informacijos saugos grėsmes ir priemones, leidžiančias išvengti informacijos saugos incidentų.

2.2.**Rizikos valdymas**. Įmonės kritinių veiklos procesų bei tinklų ir informacinių sistemų (toliau – TIS) informacijos ir kibernetinio saugumo rizika turi būti vertinama periodiškai, taip pat ir atsiradus poreikiui (kuriant naujas ar keičiant esamas informacinių technologijų sistemas, verslo procesus). Identifikuota rizika turi būti mažinama iki toleruojamo rizikos lygio taikant rizikos vertinimu pagrįstas, kainos ir

efektyvumo atžvilgiu subalansuotas bei tarptautinius informacijos saugą reglamentuojančius standartus atitinkančias informacijos saugos priemones.

Užtikrinti saugią ir patikimą informacinę ir kibernetinę įmonės aplinką, atsižvelgiant į įmonės strateginius tikslus ir neviršijant vadovybės valdomos ir prisiimamos rizikos lygio.

2.3.**Informacinis turtas.** Įmonės didžiausią vertę turintis informacinis turtas (konfidenciali informacija, komercinės paslaptys) turi būti identifikuotas bei paskirti už jį atsakingi informacinio turto savininkai. Informacinio turto savininkai turi reguliariai (ne rečiau kaip kartą per metus) peržiūrėti prie informacinio turto suteiktas prieigos teises ir imtis reikiamų veiksmų esant neatitikimų.

2.4.**Atitiktis.** Turi būti įgyvendinami įmonės vidaus bei išorės teisės aktų informacijos saugos reikalavimai, taikant rizikos vertinimu pagrįstas informacijos saugos priemones. Užtikrinti nuolatinį informacijos saugumo valdymo ciklą vadovaujantis kibernetinio saugumo įstatymu, ISO 27001 standarto reikalavimais ir kitų teisės aktų nustatytais reikalavimais, keliant informacijos saugumo tikslus, atliekant rizikos vertinimą, vidaus auditą, siekiant identifikuoti neatitiktis ir numatyti saugos gerinimo galimybes.

2.5.**Incidentų ir pažeidžiamumų valdymas**. Informacijos saugos incidentai (ir saugumo įvykiai) bei pažeidžiamumai turi būti sistemingai ir nuosekliai valdomi, užtikrinant reikiamą reagavimą, suvaldymą ir mokymąsi iš incidentų, siekiant išvengti incidentų pasikartojimo ar pažeidžiamumų išnaudojimo.

2.5.1. Bet koks informacijos saugumo normų pažeidimas laikomas informacijos saugumo incidentu, kuris gali daryti neigiamą įtaką įmonės veiklos tęstinumui, pakenkti įmonės įvaizdžiui visuomenėje ir verslo aplinkoje.

2.6.**Užtikrinti įmonės veiklos tęstinumą**, t. y. TIS, techninės ir programinės įrangos nepertraukiamą veiklą, informacijos saugumo ir kibernetinių incidentų valdymą ir informacinių sistemų veiklos atkūrimą laiku.

2.7.**Trečiųjų šalių (tiekėjų) valdymas ir priežiūra (tiekimo grandinės saugumas):**
2.7.1. Principas. Uosto direkcija taiko vieningą, dokumentuotą ir rizika pagrįstą trečiųjų šalių (tiekėjų, rangovų, paslaugų teikėjų, įskaitant subtiekėjus) valdymo ir priežiūros procesą, siekiant užtikrinti TIS, konfidencialios informacijos ir veiklos tęstinumo apsaugą viso sutarties galiojimo laikotarpiu.
2.7.2. Detalūs reikalavimai ir nuorodos. Trečiųjų šalių valdymo ir priežiūros reikalavimai (įskaitant reikalavimų nustatymą pirkimuose ir sutartyse, kvalifikacijos/pajėgumų vertinimą, prieigos valdymą, periodinę stebėseną ir kontrolę, auditą, rizikos vertinimą, incidentų ir SLA neatitikčių valdymą bei sutarties užbaigimą) nustatyti Uosto direkcijos tinklų ir informacinių sistemų kibernetinio saugumo reikalavimų aprašo (toliau – Reikalavimų aprašas) skyriuje „Tiekimo grandinės saugumas“ (toliau – TGS skyrius) ir taikomi tiesiogiai.
2.7.3. „Kritinė trečioji šalis“ – Uosto direkcijos vidaus klasifikavimo terminas trečiosioms šalims, kurių paslaugos, produktai ar suteikiamos prieigos yra reikšmingos Uosto direkcijos TIS saugai ir (ar) veiklos tęstinumui. Kritinių trečiųjų šalių atžvilgiu privalomai taikomi aktualūs TGS skyriaus reikalavimai.
2.7.4. Viršenybė. Jei Politikos nuostatos interpretuojamos kitaip nei TGS skyrius, taikomas griežtesnis reikalavimas; praktinis įgyvendinimas vykdomas vadovaujantis TGS skyriumi.

3. Dalyviai ir atsakomybės

3.1.Įmonės Stebėtojų taryba, tvirtindama Politiką, nustato informacijos saugos užtikrinimo kryptis, siekius ir principus įmonėje.

3.2.Už Politikos įgyvendinimą atsakingas Uosto direkcijos generalinis direktorius. Uosto direkcijos Veiklos atsparumo departamento vadovas užtikrina Politikos įgyvendinimo kontrolę.

3.3.Veiklos atsparumo departamentas formuoja įmonės informacijos saugos strategiją, organizuoja įmonės informacijos saugos rizikos identifikavimą, pagalbą įmonės padaliniams suvaldant riziką.

3.4.Įmonės padalinių vadovai informacijos saugos rizikos klausimus laiko neatsiejama įmonės padalinių veiklos procesų dalimi, skiria tinkamą dėmesį ir išteklius informacijos saugos rizikai valdyti.

3.5.Įmonės darbuotojai užtikrina informacijos saugumą kasdienėje veikloje priimdami sprendimus, suderintus su nuostatomis, reglamentuojančiomis informacijos saugą.

3.6.Trečiosios šalys privalo laikytis Politikos, susijusių procedūrų, standartų ir instrukcijų, taip pat galiojančių teisės aktų reikalavimų. Šis įsipareigojimas turi būti įtvirtintas sutartiniais santykiais.

3.7. Darbuotojai, inicijuojantys kritinių trečiųjų šalių pirkimus, privalo užtikrinti, kad pirkimo dokumentuose ir techninėse specifikacijose būtų nustatyti taikytini TGS skyriaus reikalavimai, kokybės vertinimo kriterijai ir SLA, ir kad sutarties sąlygos būtų suderintos su kibernetinio saugumo vadovu.
3.8. Darbuotojai, atsakingi už sutarties su kritine trečiąja šalimi įgyvendinimą, privalo vykdyti TGS skyriuje numatytą sutarties vykdymo stebėseną, fiksavimą ir eskalavimą (įskaitant incidentus ir SLA neatitiktis) bei inicijuoti sutartyje numatytas priemones, kai neatitikimai ar rizika tampa nepriimtini.
3.9.Kibernetinio saugumo vadovas (ar jo įgaliotas asmuo) privalo dalyvauti derinant kritinių trečiųjų šalių sutarčių sąlygas, turi teisę inicijuoti patikrinimus/auditus bei periodiškai vertina trečiųjų šalių incidentus ir SLA neatitiktis bei rizikos priimtinumą, vadovaujantis TGS skyriumi.

4. Politikos peržiūra ir atnaujinimas

4.1.Politika turi būti peržiūrima ne rečiau kaip kartą per metus ir, esant poreikiui, atnaujinta.

4.2.Politika tvirtinama, keičiama ar naikinama įmonės Stebėtojų tarybos sprendimu. Politiką rengia, reguliariai peržiūri ir atnaujina įmonės informacinės saugos specialistas.

4.3.Politika ir ją įgyvendinantys vidaus teisės aktai turi būti suderinti su įmonės strateginiais tikslais, tarptautiniais informacijos saugos standartais ir pasaulinėmis gerosiomis informacijos saugos praktikomis, atspindėti esamus technologinius pokyčius ir informacijos saugos grėsmių tendencijas, užtikrinti įstatymų, poįstatyminių teisės aktų ir (ar) sutartinių įsipareigojimų laikymąsi.

4.4.Politika yra skelbiama viešai įmonės interneto svetainėje www.portofklaipeda.lt ir prieinama visoms suinteresuotoms šalims.

4.5. Politikos nuostatos detalizuojamos ir įgyvendinamos priimant Uosto direkcijos informacijos saugos politiką įgyvendinančią įmonės vidaus dokumentaciją, derančią su įmonės strateginiais tikslais, teisiniais reikalavimais, tarptautiniais informacijos saugumo standartais, trečiųjų šalių reikalavimais ir gerosiomis praktikomis:

4.5.1. Tinklų ir informacinių sistemų kibernetinio saugumo reikalavimų aprašas (įskaitant skyrių „Tiekimo grandinės saugumas“), toliau – Reikalavimų aprašas;

4.5.2. Kibernetinių incidentų valdymo planas;

4.5.3. TIS įsigijimo, plėtojimo ir priežiūros saugumo, įskaitant spragų valdymą ir atskleidimą, reikalavimų aprašas;

4.5.4. TIS turto valdymo tvarkos aprašas;

4.5.5. Uosto direkcijos veiklos tęstinumo valdymo planas;

4.5.6. Kibernetinio saugumo rizikos vertinimo metodika;

4.5.7. Asmens duomenų tvarkymo taisyklės;

4.5.8. Filmavimo, fotografavimo, vaizdo ir garso duomenų tvarkymo taisyklės;

4.5.9. Informacinių ir komunikacinių technologijų naudojimo bei darbuotojų stebėsenos ir kontrolės darbo vietoje taisyklės.

_____