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)

AKCINĖS BENDROVĖS KLAIPĖDOS VALSTYBINIO JŪRŲ UOSTO DIREKCIJOS INFORMACIJOS SAUGOS POLITIKA

Tikslas:

1. Nustatyti akcinės bendrovės Klaipėdos valstybinio jūsų uosto direkcijos (toliau – įmonė arba Uosto direkcija) informacijos saugos 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:

Ši Politika taikoma visiems įmonės darbuotojams, trečiosioms šalims. 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 ypatingai 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, IT Informacijos saugos grėsmių 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 neatitikimams.

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 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.

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

3. Dalyviai ir atsakomybės

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

3.2. Už Politikos įgyvendinimą atsakingas Uosto direkcijos generalinis direktorius. Uosto direkcijos Prevencijos skyriaus vadovas užtikrina Politikos įgyvendinimo kontrolę.

3.3. Prevencijos skyrius 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. 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.

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. Šios Politikos nuostatos detalizuojamos ir įgyvendinamos priimant Politiką įgyvendinančius dokumentus, derančius su įmonės strateginiais tikslais, teisiniais reikalavimais, tarptautiniais informacijos saugumo standartais, trečiųjų šalių reikalavimais ir gerosiomis praktikomis.