PATVIRTINTA
Akcinės bendrovės „Klaipėdos nafta“
Vindikacijos vadovas
Regimantas Sriebalius
2018-03-28

INFORMACIJOS IR KIBERNETINIO SAUGUMO POLITKA

Nr. POL002

VERSIJA 1

INFORMATION AND CYBER SECURITY POLICY

TURINYS

Dokumento rengėjai:

Dr. Aidas Šmaižys, Informacinių sistemų skyriaus vadovas

Juozas Breivė, IT saugos vadovas

Kristina Kuodienė, Vyresnioji teisininkė

I. PASKIRTIS

Informacijos ir kibernetinio saugumo politika (toliau – *Politika*) yra skirta pateikti vieningus ir veiksmingus KN informacijos ir kibernetinio saugumo (toliau – *Saugumo*) valdymo principus, vadovybės poziciją informacijos ir kibernetinio saugumo atžvilgiu bei užtikrinti efektyvų KN informacijos ir kibernetinio saugumo valdymo proceso įgyvendinimą.

II. TAIKYMO SRITIS

Ši *Politika* privaloma visiems KN darbuotojams, rangovams, laikinai dirbantiems konsultantams ar kitiems KN dirbantiems asmenims, įskaitant darbuotojus, dirbančius išorės šalims ir taikoma kiekviename KN veiklos procese, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, valdomi industriniai procesai.

III. NUORODOS

Kibernetinio saugumo įstatymas – nustato kibernetinio saugumo sistemos organizavimą, valdymą ir kontrolę, apibrėžia kibernetinio saugumo politiką formuojančias ir įgyvendinančias institucijas, jų kompetenciją, funkcijas, teises ir pareigas, ypatingos svarbos informacinės infrastruktūros valdytojų pareigas bei atsakomybę ir kibernetinio saugumo užtikrinimo priemones.

Informacinės saugos reikalavimai taikomi strateginę ar svarbią reikšmę nacionaliniam saugumui turinčioms įmonėms priskirtoms energetikos ministro atsakomybei – nustato strateginę ar svarbią reikšmę nacionaliniam saugumui turinčių energetikos ministro valdymo sričiai priskirtų įmonių ir įrenginių informacinės saugos organizavimo principus, pagrindus ir pagrindinius informacinės saugos reikalavimus.

Kibernetinio saugumo reikalavimai taikomi ypatingos svarbos informacinei infrastruktūrai – nustato organizacinius ir techninius kibernetinio saugumo reikalavimus ypatingos svarbos informacinės infrastruktūros valdytojams ir viešojo administravimo subjektams, valdantiems ir (arba) tvarkantiems valstybės informacinius išteklius.

IV. SĄVOKOS IR SANTRUMPOS

Informacija – bet koks žinių elementas, pateiktas tinkama naudoti, saugoti, perduoti ar apdoroti forma. Informacija apima žodine, rašytine, audiovizualine, skaitmenine ar bet kokia kita forma išreikštus ir apibendrintus arba interpretuotus duomenis.

Informacijos saugumas – informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas. Kai tai tikslinga, papildomai gali būti įtraukti ir kiti kriterijai, tokie kaip atsakingumas, apskaita, autentiškumas/patikimumas, nepaneigiamumas ir privatumas.

Informacinė aplinka – individai (naudotojai), organizacijos ir/arba sistemos, kurios renka, apdoroja arba platina informaciją. Taip pat, ir pati informacija.

Informacinė sistema – informacijos apdorojimo sistemos ir organizacijos išteklių (pačios informacijos, žmonių, techninių priemonių, finansų ir pan.) visuma, skirta informacijai apdoroti, formuoti (kurti), skleisti (siųsti ir gauti). Tai struktūrizuotas procesų ir procedūrų rinkinys, kuriame yra kaupiami duomenys, organizuojami ir perduodami vartotojui.

Informaciniai ištekliai – informacija (duomenų bazės, duomenų rinkmenos, sutartys ir kiti dokumentai, sisteminė ir projektinė dokumentacija, mokymų medžiaga, eksploatavimo ir priežiūros procedūros, tęstinumo ir atkūrimo planai); programinė įranga (taikomoji ir sisteminė programinė

įranga, jos kūrimo priemonės); aparatinė įranga (duomenų laikmenos, organizacinė, kompiuterinė ir ryšių įranga); informacinių technologijų ir telekomunikacijų (toliau – ITT) funkcionavimui reikalingos paslaugos; išorės šalių teikiamos ITT paslaugos ir infrastruktūriniai ištekliai; darbuotojų kvalifikacija ir įgūdžiai.

Išorės šalys – paslaugų teikėjai, partneriai, klientai, kiti asmenys, turintys ar galintys turėti prieigą prie KN informacinių išteklių.

Kibernetinė aplinka – informacinių ir pramoninių procesų valdymo sistemų naudotojai, tinklai, įrenginiai, programinė įranga, perduodama arba saugoma informacija, paslaugos ir sistemos, kurios gali būti pasiekiamos elektroniniais ryšių tinklais tiesiogiai arba netiesiogiai.

Kibernetinis saugumas – reiškia KN gebėjimą kibernetinėje erdvėje apsaugoti KN elektroninį ryšių tinklą, informacinės ir pramoninių procesų valdymo sistemas bei jas apginti kibernetinių atakų atveju. Tai visuma teisinių, informacijos sklaidos, organizacinių ir techninių priemonių, skirtų kibernetiniams incidentams išvengti, juos aptikti, analizuoti ir reaguoti į juos bei įprastinei elektroninių ryšių tinklų, informacinių ir pramoninių procesų valdymo sistemų veiklai, įvykus šiems incidentams, atkurti.

Konfidencialumas – informacijos savybė, užtikrinanti jos prieinamumą tik tiems fiziniams ar juridiniams asmenims (naudotojams), kuriems tokia teisė suteikta.

Prieinamumas – informacijos savybė, garantuojanti informacijos ir jos prieigai būtinų išteklių prieinamumą sankcionuotam naudotojui reikiamu metu.

Vientisumas – informacijos savybė, nusakanti jos tikslumą ir pilnumo apsaugą bei užtikrinanti, kad informacija nebuvo atsitiktiniu ar neteisėtu būdu pakeista ar sunaikinta.

Pramoninių procesų valdymo sistema – iš informacinėmis ir ryšių technologijomis grindžiamos įrangos sudaryta sistema, skirta technologiniams procesams stebėti ar valdyti pramonės, energetikos, transporto, vandens tiekimo paslaugų ir kituose ūkinės veiklos sektoriuose.

V. POLITIKOS ĮGYVENDINIMO TIKSLAI

Saugi ir patikima informacinė ir kibernetinė KN aplinka, užtikrinanti aukštą elektroninių ryšių tinklų, informacinių ir pramoninių procesų valdymo sistemų bei informacijos saugumo lygį – tai strategiškai svarbi ir būtina sėkmingos KN veiklos ir jos tolimesnės plėtros bei KN turto ir reputacijos išsaugojimo sąlyga.

Pagrindiniai informacijos ir kibernetinio saugumo užtikrinimo tikslai:

- Užtikrinti saugią ir patikimą informacinę ir kibernetinę KN aplinką, atsižvelgiant į KN strateginius tikslus ir neviršijant *Vadovybės* valdomos bei prisiimamos rizikos lygio;
- Užtikrinti KN informacijos saugumą – t.y. KN informacijos konfidencialumą, vientisumą ir prieinamumą;
- Užtikrinti KN veiklos tęstinumą – t.y. elektroninių ryšių tinklų, informacinių ir pramoninių procesų valdymo sistemų techninės bei programinės įrangos nepertraukiamą veiklą, incidentų valdymą ir savalaikį veiklos atstatymą;
- Ieškoti naujų būdų ir priemonių, užtikrinančių saugumą, tačiau nemažinančių patogumo naudotojams ir sistemas eksploatuojančiam techniniam personalui;
- Užtikrinti ir valdyti atitikimą, informacijos ir kibernetinį saugumą bei asmens duomenų apsaugą reglamentuojančių teisės aktų reikalavimams.

VI. PAGRINDINIAI PRINCIPAI / ĮSIPAREIGOJIMAI

KN informacinės ir kibernetinės aplinkos, verslo informacinių ir pramoninių procesų valdymo sistemų saugumas yra užtikrinamas bei valdomas kuriant ir tobulinant vieningą saugumo sistemą, kurią sudaro teisinės, techninės, organizacinės bei švietimo (mokymo) priemonės, parenkamos siekiant valdyti *riziką* ir ją sumažinti iki KN vadovybei priimtino *rizikos lygio*.

KN vadovybė, siekdama užtikrinti Informacijos ir kibernetinį saugumą, nustato šiuos Informacijos ir kibernetinio saugumo valdymo principus:

- *Procesinis požiūris* – Saugumą užtikrinanti veikla KN turi būti organizuojama vadovaujantis procesiniu požiūriu. Informacijos ir kibernetinio saugumo valdymo sistemos procesų rezultatai turi būti matuojami ir periodiškai vertinami, siekiant užtikrinti nepertraukiamą procesų tobulinimą ir prisitaikymą prie besikeičiančios verslo aplinkos;
- *Darna* – informacijos ir kibernetinę saugą stiprinti sistemingai užtikrinant tolygų saugumo gerinimą visose KN veiklos srityse, nuosekliai diegiant gerąsias kibernetinio saugumo praktikas (SANS/CIS CSC20) ir nuolat identifikuojant bei stiprinant silpniausias saugumo sistemos grandis;
- *Standartizavimas* – informacijos ir kibernetinio saugumo procedūros turi būti aiškiai reglamentuotos ir visiems žinomos, valdomos pagal nustatytą vieningą standartizuotą procesą. Diegiant ir tobulinant *Saugumo* procesus turi būti siekiama vadovautis informacijos saugumo valdymo sistemos standarto (ISO 27001) reikalavimais ir ITIL metodika;
- *Prioretizavimas* – užtikrinant *Saugumą* informacinėse sistemose, saugos priemonės vertinamos sekančiais aspektais, išdėstant juos prioriteto tvarka: konfidencialumas, vientisumas, prieinamumas. *Saugumas* pramoninių procesų valdymo sistemose įgyvendinamas prioritetus nustatant sekančiai - prieinamumas, vientisumas ir konfidencialumas;
- *Klasifikavimas („Būtina žinoti")* – visa KN informacija turi būti suskirstyta pagal konfidencialumo lygius; visa nevieša informacija aiškiai pažymėta, o jos prieiga KN personalui ir trečioms šalims suteikiama tiktai griežtai vadovaujantis principu *„būtina žinoti"*;
- *Adekvatumas (saugumas prieš patogumą)* – apribojimai ir *Saugumą* užtikrinančios techninės bei organizacinės priemonės diegiamos prioretizuojant *Saugumą*, tačiau neviršijant rizikai iki KN vadovybei priimtino lygio sumažinti būtinos ribos, ir užtikrinant galimybę autorizuotam KN personalui ir išorės šalims naudotis KN skaitmeninėmis paslaugomis;
- *Racionalumas* – diegiami nauji įrankiai ir kitos techninės bei organizacinės priemonės, užtikrinančios *Saugumą* bei apsaugą nuo kibernetinių grėsmių ir pažeidžiamumų, turi atitikti saugomos informacijos vertę. Jas diegiant, vadovaujantis *Darnos* principu, įvertinami bei panaudojami turimi KN ištekliai ir kompetencijos;
- *Operatyvumas* – užtikrinamas nuolatinis informacinės ir kibernetinės aplinkos stebėjimas ir efektyvus reagavimas į kibernetinius incidentus bei informacijos ir kibernetinio saugumo incidentų (krizių) valdymas;
- *Prevencija* – didesnis dėmesys turi būti skiriamas prevencijai, o ne reagavimui į incidentus ir jų pasekmes.

Siekdama įgyvendinti nustatytus informacijos ir kibernetinio saugumo valdymo principus, KN *Vadovybė* įsipareigoja:

- Skatinti ir propaguoti incidentų prevenciją užtikrinančias priemones bei visuotinės kibernetinės higienos (sąmoningumo) ir *Saugumo* kultūrą;
- Skirti išteklius, būtinus nuolat planingai gerinti *Saugumą* užtikrinančio personalo kvalifikaciją bei įgūdžius;

– Suteikti kompetencijas ir įgaliojimus vadovams derinti bei tvirtinti su priskirtu *Saugumo* valdymo procesu susijusius dokumentus.

VII. POLITIKOS ĮGYVENDINIMAS IR KONTROLĖ

Šios *Politikos* įgyvendinimo, kontrolės, organizavimo bei užtikrinimo veiksmai ir atsakomybės aprašomos *Informacijos ir kibernetinio saugumo gairėse* bei susijusiose procedūrose.

KN *Politikos* atitikties teisės aktų reikalavimams vertinimui ir pasiūlymų dėl *Politikos* tobulinimo teikimui generalinis direktorius sudaro Saugumo komisiją, kurios uždaviniai, funkcijos ir darbo organizavimo principai apibrėžti Saugumo komisijos darbo reglamente.

Informacijos ir kibernetinio saugumo įgaliotinis ne rečiau kaip kartą per 2 (dvejus) metus turi inicijuoti vidaus patikrinimą, siekdamas nustatyti ar šį *Politika* yra tinkamai įgyvendinama praktikoje, ir parengti bei pateikti Saugumo komisijai pasiūlymus dėl šios *Politikos* pakeitimų poreikio.