Valstybinės energetikos reguliavimo tarybos
Informacijos saugumo valdymo sistemos
aprašo
1 priedas

INFORMACIJOS SAUGUMO POLITIKA

1. Informacijos saugumo politika (toliau – Politika) – tai Valstybinės energetikos reguliavimo tarybos (toliau – Taryba) pirmininko įsakymu patvirtinti dokumentai, kuriais nustatomi pagrindiniai informacijos ir asmens duomenų saugumo principai, informacijos saugumo valdymo gairės, reikalavimai informacijos saugumui užtikrinti, aprašomos šių reikalavimų įgyvendinimo procedūros, paskiriami už šių procedūrų įgyvendinimą atsakingi asmenys (nustatomos jų atsakomybės, pareigos ir funkcijos). Politikos dokumentai, kuriuose yra nustatytos organizacinės ir techninės informacijos (įskaitant asmens duomenų) saugumo valdymo priemonės, nurodyti Tarybos Informacijos saugumo valdymo sistemos aprašo 7 priede.

2. Informacija (įskaitant asmens duomenis) – tai Tarybos veiklai strategiškai svarbus turtas. Informacijos praradimas, neteisėtas atskleidimas, pakeitimas ar kiti neteisėti informacijos tvarkymo veiksmai gali sutrikdyti Tarybos veiklą. Siekiant apsaugoti Tarybos informaciją, visi Tarybos nariai, valstybės tarnautojai ir darbuotojai, dirbantys pagal darbo sutartis (toliau – Darbuotojai), Taryboje praktiką atliekantys asmenys (toliau – praktikantai), tiekėjai, teikiantys Tarybai informacinių sistemų kūrimo, modernizavimo ir (ar) priežiūros paslaugas ir kitos suinteresuotos šalys privalo vadovautis Politika.

3. Informacijos saugumas apima tris pagrindinius aspektus:

3.1. *informacijos konfidencialumą* – informacijos apsaugą nuo nesankcionuoto atskleidimo (informacija gali būti prieinama ar pateikiama (atskleidžiama) tik įgaliotiems fiziniams ar juridiniams asmenims, t. y. su informacija gali susipažinti tik tą daryti įgalioti asmenys);

3.2. *informacijos vientisumą* – informacijos apsaugą nuo nesankcionuoto ar atsitiktinio pakeitimo ar sunaikinimo;

3.3. *informacijos prieinamumą* – užtikrinimą, kad informacija gali būti tvarkoma reikiamu metu.

4. Informacijos konfidencialumą, vientisumą ir prieinamumą saugo informacijos saugumo valdymo sistema (toliau – ISVS), kuri užtikrina, kad rizikos, susijusios su informacijos saugumu Taryboje būtų tinkamai valdomos.

5. Informacijos saugumo valdymo prioritetinės kryptys:

5.1. užtikrinti tinkamą ir efektyvų informacijos saugumo valdymą ir išvengti veiklos sutrikdymo dėl informacijos konfidencialumo, vientisumo bei prieinamumo pažeidimų;

5.2. užtikrinti atitiktį teisės aktuose nustatytiems reikalavimams;

5.3. įgyvendinti gerąją praktiką atitinkančias organizacines ir technines informacijos saugumo priemones;

5.4. užtikrinti Tarybos valdomų ir (ar) tvarkomų informacinių sistemų veiklos tęstinumą;

5.5. užtikrinti efektyvų rizikos valdymą ir tinkamų rizikos valdymo priemonių naudojimą, siekiant suvaldyti riziką iki priimtino lygio.

6. Pamatuojami informacijos saugumo tikslai kiekvieniems metams nustatomi Tarybos vadovybės vertinamosios analizės metu, atsižvelgiant į informacijos saugumo valdymo prioritetines kryptis.

7. Reikalavimai informacijos saugumui nustatomi:

7.1. vadovaujantis teisės aktuose nustatytais informacijos saugos, kibernetinio saugumo ir asmens duomenų saugumo reikalavimais;

7.2. atsižvelgiant į suinteresuotų šalių keliamus reikalavimus bei lūkesčius, išreikštus informacijos saugumą, įskaitant kibernetinį saugumą ir asmens duomenų saugumą reglamentuojančiuose teisės aktuose, duomenų teikimo, tvarkymo ar kitokio pobūdžio su informacijos saugumo užtikrinimu susijusiose sutartyse, išoriniais ir vidiniais informacijos keitimosi būdais (pvz., raštais, elektroniniais laiškais ir pan.);

7.3. vadovaujantis Tarybos veiklos tikslais ir veiklos reikalavimais;

7.4. vertinant informacijos saugumo riziką.

8. Vadovybė įsipareigoja:

8.1. nustatyti informacijos saugumo valdymo tikslus;

8.2. nustatyti informacijos saugumo tobulinimo uždavinius ir priemones, įtraukiant juos į strateginį bei veiklos planus;

8.3. laikytis visų informacijos saugumo įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse;

8.4. užtikrinti efektyvų ISVS aprūpinimą reikiamais ištekliais;

8.5. sudaryti sąlygas Darbuotojams tobulinti žinias informacijos saugumo, kibernetinio saugumo ir asmens duomenų saugumo srityse.

9. Taryba nuolat gerina ISVS, įgyvendinama Politiką, informacijos saugumo valdymo tikslus, atlikdama ISVS vidaus auditus, nustatydama neatitiktis, vykdydama ISVS korekcinius veiksmus ir atlikdama vadovybės vertinamąją analizę.

10. ISVS taikoma:

10.1. visuose Tarybos veiklos procesuose, susijusiuose su saugiu informacijos tvarkymu;

10.2. visai Taryboje naudojamai informacijai (įskaitant asmens duomenis) (nepriklausomai nuo jos formato ir saugojimo būdo);

10.3. visiems Tarybos Darbuotojams, praktikantams;

10.4. visiems fiziniams ir juridiniams asmenims, kuriems teisės aktų ar sutartinių santykių pagrindu yra suteikta prieiga prie Tarybos informacijos ir (ar) informacijos apdorojimo priemonių, įskaitant informacines sistemas, tinklus ir fizinę aplinką.

11. Politika skleidžiama ISVS suinteresuotoms šalims joms prieinama ir suprantama forma. Tarybos darbuotojai ir praktikantai privalo susipažinti su Politika ir jos laikytis.