UAB „IGNITIS GRUPĖ“ ĮMONIŲ GRUPĖS INFORMACIJOS SAUGOS POLITIKA

Tikslas: Nustatyti UAB „Ignitis grupė“ Įmonių grupės informacijos saugos užtikrinimo kryptis ir principus, siekiant suvaldyti Informacijos saugos grėsmių riziką Įmonių grupėje iki toleruojamo lygio.

Taikymo sritis: UAB „Ignitis grupė“ Įmonių grupės Įmonėms.

Sąvokos ir sutrumpinimai:

Kritinis verslo procesas	Verslo procesas, kurio netekimas ar nutrūkimas Įmonei turėtų didelių finansinių, reputacinių ar reguliacinių nuostolių.
OT	Energijos gamybos ir skirstymo procesus valdančios technologijos.
Politika	Ši UAB „Ignitis grupė“ Įmonių grupės informacijos saugos politika.
Prioritetinė veikla	Įmonių grupės strateginiuose veiklos planuose įvardintos veiklos.
Trečioji šalis	Fizinis ar juridinis asmuo, kuris nepriklauso Įmonių grupei.

Kitos sąvokos ir sutrumpinimai suvokiami taip, kaip apibrėžiami Sąvokų žodyne.

1. Bendroji dalis

Informacijos vaidmuo Įmonių grupės veikloje yra ypatingai svarbus. Savalaikė Informacija padeda verslui išsiskirti ir įgyti pranašumą konkurencinėje aplinkoje. Neskiriant pakankamo dėmesio ir resursų Informacijos saugos rizikos valdymui, didėja pavojus prarasti konkurencingumą laisvoje rinkoje, patirti finansinę ir reputacinę žalą, nepasiekti Įmonėms iškeltų tikslų.

2. Informacijos saugos užtikrinimo kryptys ir principai

2.1. **Mokymai ir švietimas.** Įmonių grupėje turi būti vystoma Informacijos saugos kultūra, kad Įmonių grupės darbuotojai tinkamai suvoktų Informacijos ir jos saugos svarbą, galimą neigiamą poveikį Įmonių grupės veiklai, Įmonėms keliamų tikslų įgyvendinimui. Turi būti nuolatos didinamas visų Įmonių grupės darbuotojų atsparumas Informacijos saugos grėsmėms periodiškai organizuojant mokymus, tikrinant darbuotojų žinias, vykdant nuolatinę komunikaciją apie Įmonių grupei aktualias Informacijos saugos grėsmes ir priemones leidžiančias išvengti Informacijos saugos Incidentų.

2.2. **Rizikos valdymas.** Įmonių grupės svarbiausių veiklos procesų, IT ir OT Informacijos saugos grėsmių rizika turi būti vertinama periodiškai, taip pat ir atsiradus poreikiui (kuriant naujas ar keičiant esamas IT, OT sistemas, IS, 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 (ISO 27001, IEC 62443) atitinkančias Informacijos saugos priemones.

2.3. **Informacinis turtas.** Įmonių grupės didžiausią vertę turintis Informacinis turtas (Įmonių 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 Įmonių grupės Įmonių sutartiniai įsipareigojimai su Trečiosiomis šalimis, Įmonių grupės vidaus bei išorės teisės aktų Informacijos saugos reikalavimai (atsižvelgiant į šalies, kurioje Įmonių grupės Įmonė vykdo veiklą), taikant rizikos vertinimu pagrįstas Informacijos saugos priemones.

2.5. **Santykiai su Trečiosiomis šalimis.** Informacijos, kuria keičiamasi su Trečiųjų šalių partneriais, tiekėjais, saugumas turi būti užtikrintas visu sutarčių galiojimo metu, į sutartis siekiant įtraukiant Informacijos saugos nuostatas, įpareigojančias Informacijos gavėjus užtikrinti ne mažesnį Informacijos saugos lygį, nei kad taikomas Įmonių grupėje.

2.6. **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.

2.7. **Aiški savininkystė.** Įmonių grupėje turi būti paskirti IT paslaugų ir sistemų, OT įrenginių, Kritinių verslo procesų savininkai (turintys sprendimų teisę ir valdantys reikalingus išteklius), atsakingi už tinkamą Informacijos saugos ir Kibernetinių grėsmių rizikos valdymą.

3. Dalyviai ir atsakomybės

3.1. **Bendrovės valdyba** tvirtindama šią politiką nustato Informacijos saugos užtikrinimo kryptis, siekius ir principus Įmonių grupėje.

3.2. **Informacijos saugos funkcijos vadovas** formuoja Įmonių grupės Informacijos saugos strategiją, organizuoja Įmonių grupės Informacijos saugos rizikos identifikavimą, pagalbą Įmonėms suvaldant riziką, tvirtina Politikos įgyvendinimo gaires, kontroliuoja jų įgyvendinimą.

3.3. **Įmonių vadovai** Informacijos saugos rizikos klausimus laiko neatsiejama Įmonės veiklos procesų dalimi, skiria tinkamą dėmesį ir išteklius Informacijos saugos rizikos valdymui.

3.4. **Įmonių grupės darbuotojai** užtikrina Informacijos saugumą kasdienėje veikloje priimdami sprendimus, suderintus su nuostatomis reglamentuojančiomis Informacijos saugą.

4. Politikos peržiūra ir atnaujinimas

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

4.2. Politika ir ją įgyvendinantys vidaus teisės aktai turi būti suderinti su Įmonių grupės strateginiais tikslais ir Prioritetinėmis veiklomis, tarptautiniais Informacijos saugos standartais (ISO 27001, IEC62443) 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.