

INFORMACIJOS SAUGOS VADOVAS

1. Informacijos saugos vadovas (toliau – Saugos vadovas) yra pagrindinis UAB „Investicijų ir verslo garantijos“ (toliau – INVEGA) informacijos saugumo dokumentas. Saugos vadovą įsakymu tvirtina INVEGA direktorius. Šio dokumento dalys gali būti pateikiamos susipažinti su INVEGA informacija susijusioms šalims, joms prieinama ir suprantama forma.

2. Saugos vadovo tikslas – pateikti INVEGOS direktoriaus poziciją informacijos saugumo atžvilgiu bei apsaugoti visą INVEGOS gaunamą, siunčiamą, kuriamą, valdomą ir naudojamą žodinę, rašytinę ir elektroninę informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos INVEGOS vykdomai veiklai ir įvaizdžiui.

3. Įgyvendinant Saugos vadovo tikslą yra siekiama tokių informacijos saugumo uždavinių:

3.1. užtikrinti ir valdyti informacijos saugumą, atsižvelgiant į INVEGOS veiklos (strateginius) tikslus duomenų centro ir IT paslaugų srityje;

3.2. užtikrinti ir valdyti atitikimą išoriniams ir vidiniams informacijos saugumo reikalavimams, atliekant periodinį atitikties vertinimą ir šalinant nustatytus trūkumus;

3.3. užtikrinti informacijos saugumo pažeidimų sprendimą ir jų priežasčių pašalinimą, įgyvendinant informacijos saugos incidentų valdymo procesą;

3.4. užtikrinti tinkamą informacijos saugumo ir apdorojimo priemonių parinkimą ir įgyvendinimą, atliekant kasmetinį rizikos vertinimą ir įgyvendinant Rizikos valdymo planą;

3.5. užtikrinti taikomų informacijos saugumo priemonių veiksmingumą;

3.6. užtikrinti Veiklos tęstinumo valdymo plano tinkamumą, atliekant jo periodinę peržiūrą ir testavimą.

4. **Informacija** – tai strategiškai svarbus INVEGOS turtas, kurio praradimas, neteisėtas paviešinimas, pakeitimas ar sugadinimas gali sukelti veiklos sutrikimų ir dėl to INVEGA ar subjektai, kurių duomenis kaupia ir saugo INVEGA, gali patirti nuostolių. Informacija gali būti spausdinta, rašyta, garsinė ar vaizdinė. Informacija gali būti saugoma ne tik popieriniame pavidale, bet ir elektroniniame, siunčiama paštu arba elektroninių priemonių pagalba, ar minima spaudoje ar pokalbyje.

5. Saugos vadove išdėstytos nuostatos yra taikomos visiems INVEGOS veiklos procesams ir apima visus informacijos resursus: žodinę bei rašytinę informaciją, informacines sistemas, kompiuterių tinklus, fizinę aplinką, INVEGOS darbuotojus, bet kuriuos fizinius ir juridinius asmenis, pasirašiusius su INVEGA bendradarbiavimo sutartis, kuriems suteikta prieiga prie INVEGOS valdomos informacijos ir jos apdorojimo, perdavimo ir (ar) saugojimo priemonių. Informacijos tvarkymas yra bet kuris su INVEGOS disponuojama informacija atliekamas veiksmas: rinkimas, užrašymas, kaupimas, saugojimas, klasifikavimas, grupavimas, jungimas, keitimas, teikimas, paskelbimas, naudojimas, loginės ir (ar) aritmetinės operacijos, paieška, skleidimas, naikinimas ar kitoks veiksmas arba veiksmų visuma. INVEGOS darbuotojams šis Saugos vadovas yra taikomas ir privalomas.

6. Informacijos saugumas apima tris pagrindinius aspektus:

6.1. informacijos konfidencialumas – informacijos apsauga nuo nesankcionuoto atskleidimo;

6.2. vientisumas – informacijos apsauga nuo nesankcionuoto ar atsitiktinio pakeitimo;

6.3. prieinamumas – užtikrinimas, kad informacija yra prieinama tada, kai ji reikalinga tinkamai vykdyti INVEGA veiklą.

7. Saugos vadovas:

7.1.1. aprašo INVEGA saugumo politiką, skirtą apsaugoti jos ir klientų informacinio turto, t. y. bet kokios formos informacijos, taip pat su ja susijusio materialaus (kompiuterių bei ryšio įrenginių, patalpų ir pan.) bei nematerialaus (reputacijos, įvaizdžio) turto konfidencialumą, vientisumą ir prieinamumą;

7.1.2. nustato atsakomybę už informacijos saugumą;

8. Saugos vadovas turi būti peržiūrima ne rečiau kaip kartą per metus.

9. INVEGA informacijos saugumo reikalavimų įgyvendinimas vadovaujantis atsižvelgiant į tarptautinio standarto ISO/IEC 27001 reikalavimus ir nacionalinius teisės aktus, reglamentuojančius informacijos saugą ir kibernetinį saugumą.

10. Informacijos saugumo valdymas INVEGA yra pagrįstas rizikos valdymu. Informacijos saugumo rizikos vertinimas sudaro sąlygas, kad informacijos saugumo valdymo priemonės, taikomos INVEGA veikloje,

atitiktų pagrindinius INVEGA veiklos ir informacijos saugumo tikslus. Rizikos valdymo procesas turėtų apimti visas reikšmingas INVEGOS veiklos sritis ir nustatyti bei valdyti tikėtinas rizikas – strateginę, finansinę, operacinę, atitikties, reputacinę, kurios gali neigiamai paveikti INVEGOS veiklą.

11. INVEGA informacijos saugumo rizika vertinama kas 2 kalendorinius metus pagal patvirtintą Informacijos saugumo rizikos valdymo metodiką.

12. Invega informacijos saugumo valdymas užtikrina tarptautinių ir LR teisės aktų, reglamentuojančių informacijos saugą ir kibernetinį saugumą bei asmens duomenų apsaugą, reikalavimų įgyvendinimą.
