INFORMACIJOS SAUGUMO POLITIKA

PRIORITETAS	Informaciją laikome prioritetiniu mūsų veiklos ištekliu, todėl elektroninės, rašytinės, žodinės informacijos saugumas yra esminis siekis, norint užtikrinti uždarosios akcinės draudimo brokerio bendrovės „IVP Partners“ (toliau – Bendrovės) patikimumą, finansinį stabilumą, veiklos tęstinumą ir suinteresuotų šalių reikalavimų vykdymą.
TIKSLAS	Informacijos saugumo politika (toliau – Politika) apibrėžia Bendrovės vadovybės poziciją ir atsakomybę informacijos ir kibernetinio saugumo srityje. Ji yra skirta pateikti vieningus saugumo valdymo principus bei užtikrinti efektyvų Bendrovės informacijos saugumo valdymo proceso įgyvendinimą.
TAIKYMO SRITIS	Ši Politika privaloma visiems Bendrovės darbuotojams, akcininkams ir vadovybei, įskaitant laisvai samdomus specialistus – paslaugų teikėjus. Politika taikoma kiekvienoje Bendrovės lokacijoje, veikloje ir procese, kur yra valdoma, perduodama ar kitaip tvarkoma informacija, nepriklausomai nuo jos formos ir saugojimo būdo.
VALDYMO SISTEMA	Informacijos saugos valdymą Bendrovė vykdo remdamasi tarptautinio standarto ISO/IEC 27001:2017 reikalavimais, kurių vykdymą kasmet patikrina ir patvirtina išorinis auditorius - sertifikavimo viešoji įstaiga „LST Sert“ (juridinio asmens kodas – 300076307).
UŽTIKRINIMO KRYPTYS	Užtikrinti saugią ir patikimą informacinę ir kibernetinę Bendrovės aplinką, atsižvelgiant į Bendrovės strateginius tikslus ir neviršijant vadovybės valdomos ir prisiimamos rizikos lygio. Užtikrinti Bendrovės veiklos tęstinumą, t.y. elektroninių ryšių tinklų, informacinių sistemų, techninės ir programinės įrangos nepertraukiamą veiklą, informacijos saugumo ir kibernetinių incidentų valdymą ir savalaikį veiklos atstatymą. Užtikrinti nuolatinį informacijos saugumo valdymo ciklą, vadovaujantis EN ISO/IEC 27001:2017 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.

PRINCIPAI

Padidintas dėmesys informacijos ir kibernetinio saugumo kultūros vystymui ir palaikymui. Darbuotojai yra edukuojami tinkamai suvokti informacijos ir jos saugumo svarbą, galimą neigiamą poveikį Bendrovės veiklai, keliamų strateginių tikslų įgyvendinimui. Nuolatos didinamas visų Bendrovės darbuotojų atsparumas bei sąmoningumas kibernetinėms grėsmėms periodiškai organizuojant mokymus, vykdant nuolatinę komunikaciją apie aktualias grėsmes ir priemones, leidžiančias išvengti incidentų.

Rizikos vertinimas ir valdymas. Bendrovės svarbiausių veiklos procesų ir informacijos laikymo šaltinių su įvairiomis galimomis grėsmėmis ryšiai yra vertinami periodiškai. Identifikuota rizika mažinama iki toleruojamo rizikos lygio taikant rizikos vertinimu pagrįstas, kainos ir efektyvumo atžvilgiu subalansuotas saugumo priemones.

Atitiktis. Užtikrinti atitiktį teisės aktuose nustatytiems informacijos ir kibernetinio saugumo reikalavimams, Bendrovės sutartiniams įsipareigojimams su trečiosiomis šalimis: partneriais, draudikais bei klientais.

Sistemingas incidentų ir pažeidžiamumų valdymas. Valdant informacijos saugumo ir kibernetinius incidentus, užtikrinamas reikiamas reagavimas, suvaldymas ir incidentų prevencija ateityje.

Testavimas. Vykdomas kasmetinis vidinis ir išorinis sistemų testavimas, užtikrinantis kuo mažesnę pažeidžiamumų tikimybę.

ATSAKOMYBĖ

Bet koks Informacijos saugumo normų pažeidimas laikomas Informacijos saugumo incidentu, kuris gali daryti neigiamą įtaką Bendrovės veiklos tęstinumui, sugadinti ir pakenkti Bendrovės įvaizdžiui visuomenėje ir verslo aplinkoje.

Nedelsiant pranešti pastebėjus Bendrovės informacinių sistemų veiklos sutrikimą ar saugumo incidentą, kibernetinio saugumo spragą ar silpnąją vietą Bendrovės vadovybei el. paštu info@ivp.lt arba telefonu +370 5 219 7601.

Bendrovės darbuotojams ir trečiosioms šalims, pažeidusiems informacijos saugumo vadybos sistemos reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose, Bendrovės vidaus teisės aktuose bei sutartyse, susitarimuose ar kituose teisinę galią turinčiuose dokumentuose numatytos poveikio priemonės.

ĮSIPAREIGOJIMAI	Laikytis visų informacijos ir kibernetinio saugumo įsipareigojimų, reglamentuotų Europos Sąjungos ir Lietuvos Respublikos teisės aktuose bei sutartyse ir prižiūrėti ir nuolat tobulinti informacijos saugumo valdymo sistemos efektyvumą.
POLITIKOS PERŽIŪRA IR SKLAIDA	Politika tvirtinama, keičiama ar naikinama Bendrovės vadovybės sprendimu. Politiką rengia, reguliariai peržiūri ir atnaujina Bendrovės informacinės saugos specialistas. Politika yra skelbiama viešai Bendrovės interneto svetainėje www.ivp.lt ir prieinama visoms suinteresuotoms šalims. Šios Politikos nuostatos detalizuojamos ir įgyvendinamos priimant Bendrovės vidaus dokumentaciją, derančią su Bendrovės strateginiais tikslais, teisiniais reikalavimais, tarptautiniu informacijos saugumo standartu, trečiųjų šalių reikalavimais ir gerosiomis praktikomis.

Patvirtinta: 2023 09 22, versija Nr. 3