INFORMACIJOS
SAUGUMO POLITIKA

SAUGUMO POLITIKOS TIKSLAI

Pagrindinis mūsų tikslas - užtikrinti visišką savo ir klientų duomenų konfidencialumą, vientisumą ir prieinamumą, kad mūsų veikla vyktų sklandžiai. Šia politika visiems verslo partneriams, darbuotojams, visuomenei ir valstybės administracijai bei plačiajai visuomenei deklaruojame „Skrivanek Holding SE“ gebėjimą veiksmingai apsaugoti mums priklausančią ir patikėtą informaciją, materialųjį ir nematerialųjį turtą pagal teisės aktų reikalavimus kiekvienoje šalyje, kurioje vykdome veiklą.

INFORMACIJOS SAUGUMO PRINCIPAI 1/3

Įsipareigojame: laikytis ir palaikyti teisės aktų informacijos saugumo srities teisės aktus visose šalyse, kuriose veikia mūsų grupė, užtikrinti, kad galimybę laiku ir konkrečioje vietoje gauti informacijos pagal visuomenės poreikius, tačiau šią informaciją teikti tik tiems, kurie tik tiems, kuriems ji reikalinga jų darbui, taip išlaikant informacijos konfidencialumą pagal nustatytas kategorijas - viešoji, vidinė, konfidenciali, asmeninė.

SKRIVANEK

VALDYMO PAREIŠKIMAS

„Skrivanek“ yra pirmaujanti kalbų vertimo raštu ir žodžiu, lokalizavimo, DTP paslaugų ir kalbų mokymo paslaugų teikėja Čekijoje ir dar 13 pasaulio šalių.

„Skrivanek Holding SE“ vadovybė skelbia šią Informacijos saugumo politiką kaip pagrindą, kuriuo vadovaujasi Bendrovė informacijos saugumo apsaugos srityje. Vadovybė ketina remti šioje politikoje nustatytus tikslus ir principus.

INFORMACIJOS SAUGUMO PRINCIPAI 2/3

Taip pat įsipareigojame: valdyti informacijos vientisumą ir gyvavimo ciklą nuo jos sukūrimo, perdavimo ir naudojimo iki sunaikinimo, mokyti ir tobulinti savo darbuotojus, tiekėjus ir partnerius informacijos saugumo srityje, o informacijos saugumo taisyklių pažeidimas laikomas šiurkščiu vidaus taisyklių ir sutartinių santykių pažeidimu.

SAUGUMO POLITIKOS SERTIFIKAVIMAS

Siekdama įgyvendinti šią politiką, Bendrovė įdiegė ir sukūrė informacijos saugumo valdymo sistemą pagal ISO/IEC 27001:2022 standartą. Tai tarptautinis informacijos saugumo valdymo sistemų standartas. Juo užtikrinama apsauga nuo galimų saugumo grėsmių, tokių kaip kibernetiniai nusikaltimai, piktnaudžiavimas asmens duomenimis, vandalizmas ir (arba) terorizmas, gaisras ir (arba) sugadinimas, netinkamas naudojimas ir duomenų vagystė / virusų ataka.

INFORMACIJOS SAUGUMO PRINCIPAI 3/3

Be to, įsipareigojame: nustatyti saugumo priemones pagal rizikos rimtumo, jos poveikio ir ekonominio poveikio įvertinimo principą, reguliariai stebėti, iš naujo vertinti riziką, valdyti saugumo įvykius ir incidentus taikant korekcines ir prevencines priemones, kad padidintume savo informacijos saugumo valdymo sistemos veiksmingumą.

2020 - **2024**

Suggested: OLO Approved: BCH 2. 1. 2024