INFORMACIJOS SAUGUMO POLITIKA

SAUGUMO POLITIKOS TIKSLAI

Pagrindinis mūsų tikslas – užtikrinti sklandžiai verslo veiklai būtiną visų savo ir klientų duomenų konfidencialumą, vientisumą ir prieinamumą. Remdamiesi šia politika, visiems verslo partneriams, darbuotojams, visuomeninėms ir valstybės institucijoms bei plačiajai visuomenei patvirtiname, kad UAB „Skrivanek vertimų biuras“ turi galimybę veiksmingai apsaugoti įmonei priklausančią ir jai patikėtą informaciją, materialųjį ir nematerialųjį turtą remdamasi visų šalių, kurioje įmonė dirba, įstatymų reikalavimais.

1-ASIS INFORMACIJOS SAUGUMO PRINCIPAS

Įsipareigojame:

laikytis informacijos saugumą reglamentuojančių teisės aktų ir juos įgyvendinti visose šalyse, kuriose veikia mūsų įmonių grupė, užtikrinti, kad informacija būtų pasiekiama visuomenės pageidaujamu metu ir vietoje, tačiau teikti šią informaciją tik tiems, kuriems jos reikia darbui atlikti, ir taip laikytis informacijos konfidencialumo reikalavimų atsižvelgiant į konkrečias – viešos, vidinės, konfidencialios, asmeninės – informacijos kategorijas.

SKRIVANEK

VADOVYBĖS PAREIŠKIMAS

„Skrivanek“ yra viena didžiausių kalbinių paslaugų vertimų žodžiu ir raštu, lokalizacijos, maketavimo ir kalbų mokymo srityje teikėja Lietuvoje ir dar 13 kitų pasaulio šalių.

„Skrivanek“ vadovybė informuoja, kad remiantis šia Informacijos saugumo politika nustatoma, kaip įmonė užtikrina informacijos saugumą. Vadovybė siekia įgyvendinti nustatytus šios politikos tikslus ir principus.

2-ASIS INFORMACIJOS SAUGUMO PRINCIPAS

Taip pat įsipareigojame:

valdyti informacijos vientisumą ir gyvavimo ciklą nuo jos sukūrimo, perdavimo ir naudojimo iki jos pašalinimo,

mokyti ir ugdyti savo darbuotojus, tiekėjus ir partnerius informacijos saugumo srityje, kad jie suprastų, jog informacijos saugumo taisyklių pažeidimas laikomas šiurkščiu vidaus taisyklių ir sutartinių teisių pažeidimu.

SAUGUMO POLITIKOS SERTIFIKAVIMAS

Siekdama įgyvendinti politiką, įmonė įdiegė ir išplėtojo informacijos saugumo valdymo sistemą pagal ISO/IEC 27001: 2013 – tarptautinį informacinių saugumo valdymo sistemų sertifikavimo standartą. Tai suteikia apsaugą nuo tokių galimų grėsmių saugumui kaip elektroniniai nusikaltimai, netinkamas asmens duomenų naudojimas, vandalizmas, terorizmas, gaisras, žala, piktnaudžiavimas ir duomenų vagystė, virusai.

TÜV NORD
TÜV NORD CERT GmbH
ISO 27001

3-IASIS INFORMACIJOS SAUGUMO PRINCIPAS

Be to, įsipareigojame:

nustatyti apsaugos priemones, grindžiamas rizikos pavojingumo, poveikio ir ekonominio veiksmingumo vertinimo, nuolatinės stebėsenos ir pakartotinio rizikos vertinimo principu;

valdyti saugumo įvykius ir incidentus naudojant taisomąsias ir prevencines priemones ir taip padidinti savo informacijos saugumo valdymo sistemų veiksmingumą.

2020 - 2024