Informacijos saugumo politika (2025 – 2027)

Vadovybės pareiškimas

„Skrivanek“, kaip pirmaujantis kalbų technologijų paslaugų teikėjas, skelbia šią Informacijos saugumo politiką kaip pagrindą verslo operacijų apsaugai ir suinteresuotųjų šalių pasitikėjimui užtikrinti.

Įgyvendindami ir nuolat tobulindami savo Informacijos saugumo valdymo sistemą (ISVS), atitinkančią ISO/IEC 27001:2022 standartą, siekiame:

- Apsaugoti nuo kylančių grėsmių, įskaitant kibernetinį nusikalstamumą, dirbtinio intelekto keliamas rizikas ir netinkamą duomenų naudojimą.
- Užtikrinti atitiktį taikomiems tarptautiniams ir vietos teisės aktams, laikantis aktyvaus požiūrio į jų pokyčius.
- Puoselėti saugumo kultūrą visais organizacijos lygmenimis.
- Vadovybė remia šią politiką, teikdama išteklius, lyderystę ir strateginę priežiūrą, siekdama užtikrinti jos įgyvendinimą, reguliarią peržiūrą ir suderinamumą su pasaulinėmis gerosiomis praktikomis.

Saugumo politikos tikslai

- Stiprinti priemones, skirtas kovoti su kylančiomis kibernetinio saugumo grėsmėmis, įskaitant išpirkos reikalaujančias programas (ransomware), sukčiavimą (phishing) ir dirbtinio intelekto pagrįstas atakas.
- Gerinti atitiktį pasauliniams ir regioniniams duomenų apsaugos reglamentams (pvz., BDAR, CCPA ir naujiems vietiniams reikalavimams).
- Nuolat tobulinti rizikos vertinimo ir incidentų valdymo procesus, siekiant juos suderinti su geriausiomis informacijos saugumo praktikomis.
- Skatinti saugumo sąmoningumo kultūrą tarp darbuotojų, tiekėjų ir partnerių.

Principai

Mes įsipareigojame:

- Laikytis ir užtikrinti informacijos saugumo teisės aktų laikymąsi visose šalyse, kuriose veikia mūsų grupė.
- Užtikrinti informacijos prieinamumą verslo operacijoms reikiamu laiku ir vietoje, tuo pat metu ribojant prieigą pagal mažiausios privilegijos principą.
- Klasifikuoti ir tvarkyti informaciją kaip viešą, vidinę, konfidencialią ar asmeninę, taikant griežtą prieigos kontrolę kiekviename lygyje.
- Stiprinti prieigos valdymo protokolus, naudojant daugiafaktorinę autentifikaciją (MFA) ir vaidmenimis pagrįstą prieigos kontrolę (RBAC), siekiant sumažinti neteisėtos prieigos riziką.
- Valdyti informacijos vientisumą ir gyvavimo ciklą – nuo jos sukūrimo ir perdavimo iki saugaus sunaikinimo, užtikrinant, kad visi procesai atitiktų tarptautinius standartus.
- Nuolat vykdyti reguliarius mokymus ir įgyvendinti privalomas kasmetines programas, pritaikytas pagal darbo funkcijas, orientuotas į naujas grėsmes ir saugų duomenų tvarkymą, siekiant organizacijos mastu didinti informuotumą ir pasirengimą.
- Informacijos saugumo taisyklių pažeidimus laikyti šiurkščiais vidinių reglamentų ir sutarčių pažeidimais.
- Nustatyti saugumo priemones atsižvelgiant į rizikos rimtumą, jų poveikį ir kaštų efektyvumą, užtikrinant proporcingą ir pritaikomą saugumą.
- Reguliariai stebėti rizikas, iš naujo vertinti grėsmes ir taikyti korekcines bei prevencines priemones, siekiant nuolat tobulinti informacijos saugumo valdymo sistemą (ISVS).
- Plėsti incidentų reagavimo pajėgumus, įskaitant realaus laiko aptikimo, ataskaitų teikimo ir žalos mažinimo strategijas, siekiant sumažinti prastovų laiką ir poveikį.
- Integruoti dirbtiniu intelektu grįstas grėsmių aptikimo ir reagavimo sistemas, leidžiančias greičiau identifikuoti ir suvaldyti saugumo pažeidimus, taip stiprinant bendrą mūsų informacijos saugumo sistemą.

Parengė: Anna Julie Skrivankova, 10.04.2025