

INFORMACIJOS SAUGUMO POLITIKA

UAB „LEXNET“ Informacijos saugumo valdymo sistema (toliau — ISVS) taikoma kuriant informacines sistemas ir projektuojant programinę įrangą, jas tobulinant ir parduodant bei atliekant informacinių sistemų ir programinės įrangos priežiūrą.

Bendrasis ISVS informacijos saugumo tikslas – pasiekti ir palaikyti UAB „LEXNET“ nustatytą informacijos saugumo lygį išlaikant tinkamą informacijos konfidencialumą, vientisumą ir prieinamumą, taip pat užtikrinti ilgalaikį klientų pasitikėjimą. Informacijos saugumo politikos tikslas: apibrėžti bendrusius informacijos saugos reikalavimus, kurie atitiktų UAB „LEXNET“ strategiją, verslo poreikius ir galiojančius teisės aktus, bei užtikrinti UAB „LEXNET“ informacinių vertybių apsaugą nuo vidinių ar išorinių, tyčinių ar atsitiktinių grėsmių. Informacijos saugumo politika – tai bendrasis planas, kuris apibrėžia tikslus ir siekiamybes, kurias turi užtikrinti IT saugumo taisyklės ir procedūros. Visos UAB „LEXNET“ instrukcijos, tvarkos ir procedūros, susijusios su informacijos saugojimu, apdorojimu ir platinimu Įmonės aplinkoje, o taip pat trečiosioms šalims, yra rengiamos vadovaujantis šia Informacijos saugumo politika.

Informacijos saugumo politika yra pirmiausiai grindžiama rizika pagrįstu požiūriu. UAB „Lexnet“ vykdomos informacijos saugumo rizikos informacinėse sistemose valdymo procesas (poveikio įmonės veiklai analizė, grėsmių analizė, rizikos lygio nustatymas, rizikos priimtimumo nustatymas, taikytinų saugumo priemonių parinkimas, rizikos valdymo plano rengimas ir jo priežiūra) reglamentuotas Informacijos saugumo rizikos valdymo apraše.

Siekiant šių tikslų UAB „LEXNET“ laikosi žemiau įvardintų Informacijos saugumo politikos nuostatų:

- ISVS reikalavimai informacijos saugumui taikomi bet kokiai informacijai, nepriklausomai nuo to, kur ji yra, kokioje laikmenoje ji saugoma, kokios technologijos naudojamos jai apdoroti ir kokie žmonės ją tvarko bei apdoroja.
- ISVS reikalavimai taikomi visiems UAB „LEXNET“ padaliniais ir veiklos procesams.
- ISVS atsižvelgta į veiklos ir teisinius ar reglamentų reikalavimus bei sutartyse numatytus saugumo įsipareigojimus.
- Bet koks Informacijos saugumo normų pažeidimas laikomas Informacijos saugumo incidentu, kuris gali neigiamai įtakoti UAB „LEXNET“ veiklos tęstinumą bei sugadinti organizacijos įvaizdį visuomenėje.
- UAB „LEXNET“ darbuotojams ar trečiosioms šalims, sąmoningai ar nesąmoningai pažeidusiems Informacijos saugumo politikos reikalavimus, yra taikomos Lietuvos Respublikos įstatymuose (pavyzdžiui, Asmens duomenų teisinės apsaugos įstatyme) numatytos priemonės.

- Periodiškai atliekama vadovybės analizė užtikrina nuolatinį ISVS tinkamumą, adekvatumą, rezultatyvumą ir plėtrą.
- Informacijos saugumo politika reguliariai peržiūrima (ne rečiau kaip vieną kartą per metus), atnaujinama pagal peržiūros rezultatus. Informacijos saugumo politika atnaujinama tuojau pat, jeigu įvyko svarbūs pasikeitimai UAB „LEXNET“ IT infrastruktūroje. Atnaujinant Informacijos saugumo politiką atsižvelgiama į metinės rizikos analizės rezultatus, t.s. į žalą veiklai, kurią sukėlė ar gali sukelti informacijos saugumo pažeidimai.
- Informacijos saugumo politika skelbiama viešai.