INFORMACIJOS SAUGOS POLITIKA			
Organizacija	**Proitas, UAB**	**Versija**	**2.0**

INFORMACIJOS SAUGOS POLITIKA

Šiame dokumente Proitas, UAB (toliau – Bendrovė) apibrėžia patvirtintą ir taikomą informacijos saugos politiką. Bendrovė siekia užtikrinti savo verslo ir teikiamų paslaugų įskaitant ir sistemos CMonitor nepertraukiamą veiklą, apsaugas nuo informacijos nutekėjimo bei duomenų pakeitimo.

Siekdama užtikrinti stabilų ir saugų veikimą, Bendrovė įdiegė informacijos saugumo valdymo sistemą (ISVS) pagal tarptautinį informacijos saugos standartą ISO/IEC 27001:2022. Šis standartas nustato ISVS reikalavimus, remiantis geriausiomis tarptautinėmis praktikomis, galiojančiais įstatymais bei klientų reikalavimais. .

Bendrovė yra įsipareigojusi palaikyti pilną ISO/IEC 27001:2022 sertifikavimą įtraukiant visas nustatytas kontrolės priemones. Siekiant įvertinti kontrolės priemonių veikimą Bendrovė į ISVS patikrinimą įtraukia nepriklausomą sertifikavimo įstaigą kuri kiekvienais metais atlieka išorinius patikrinimo auditus

Ši politika taikoma visoms Bendrovės informacinėms sistemoms, žmonėms ir procesams, įskaitant vadovybę, darbuotojus, tiekėjus ir kitas trečiąsias šalis, turinčias prieigą prie įmonės sistemų ir duomenų.

2. Informacijos saugumo reikalavimai

Informacijos saugumo reikalavimai Bendrovėje yra aiškiai apibrėžti ir nuolat peržiūrimi, siekiant atitikti vidinius verslo poreikius bei debesijos paslaugų klientų reikalavimus. Be to, dokumentuojami ir įgyvendinami visi teisės aktų, reguliacinių institucijų ir sutarčių reikalavimai.

3. Informacijos saugumo tikslai

Bendrovėje kasmet nustatomi aiškūs informacijos saugos tikslai, kurie susieti su biudžeto planavimo ciklu, taip užtikrinant finansavimą identifikuotiems tobulinimo veiksmams. Tikslai nustatomi remiantis verslo poreikių analize, rizikų vertinimais bei suinteresuotų šalių nuomonėmis. Jie yra dokumentuojami, peržiūrimi ir vertinami valdymo peržiūros metu.

4. Nuolatinis ISVS tobulinimas

Bendrovė įsipareigoja nuolat gerinti ISVS efektyvumą ir siekia:

- Tobulinti esamus procesus pagal ISO/IEC 27001:2022 geriausias praktikas;
- Pasiekti ir palaikyti ISO/IEC 27001:2022 sertifikavimą;
- Didinti informacijos saugumo priemonių matomumą ir valdymo efektyvumą;
- Kasmet peržiūrėti saugos rodiklius ir atnaujinti juos pagal istorinius duomenis;
- Reguliariai peržiūrėti ir įgyvendinti saugos tobulinimo idėjas, gautas iš darbuotojų, klientų, tiekėjų ir IT specialistų.

5. Politikos įgyvendinimas

Ši politika yra patvirtintą Bendrovės aukščiausios vadovybės bei privalo būti laikomasi visų darbuotojų. Politikos nesilaikymas gali sukelti drausmines priemones, įskaitant įspėjimus, darbo ar paslaugų teikimo sutarties nutraukimą. Visi klausimai, susiję su informacijos saugos politika, turėtų būti adresuojami privacy@proitas.lt

Bendrovės vadovybė įsipareigoja nuolat peržiūrėti ir atnaujinti šią politiką, siekiant užtikrinti jos veiksmingumą ir atitikimą naujausiems saugumo standartams.

TVIRTINU

_____ _____ _____

(Pareigos) (Parašas) (Vardas ir pavardė)