



## UAB LINEV SYSTEMS EU

PATVIRTINTA  
LINEV Systems EU UAB  
Direktorius  
2026 m. Kovo 09 d. įsakymu Nr.2026/01

### INFORMACIJOS SAUGUMO POLITIKA

**Politikos tikslas:** Nustatyti privalomus informacijos saugumo valdymo principus, remiantis ISO/IEC 27001:2022, visose įmonės veiklos srityse.

**Politikos taikymo sritis:** Ši informacijos saugumo politika taikoma visiems UAB LINEV Systems EU darbuotojams ir yra privaloma.  
Politika taikoma visoje įmonės veikloje, įskaitant:

- Rentgeno, jonizuojančios ir elektromagnetinės spinduliuotės instrumentų ir įrangos projektavimą;
- Įrangos kūrimą, gamybą, montavimą ir priežiūrą.

Įmonės pagrindinis tikslas – apsaugoti įmonės ir klientų informaciją bei duomenis. Darbuotojai vadovaujasi ISO/IEC 27001:2022 standarto reikalavimais, siekdami užkirsti kelią saugumo incidentams, galintiems pakenkti įmonės reputacijai.

UAB LINEV Systems EU vadovybė taiko šiuos **įsipareigojimus**:

- Užtikrinti įmonės informacijos ir informacinių technologijų išteklių konfidencialumą, vientisumą ir prieinamumą.
- Užtikrinti atitiktį informacijos saugumo reikalavimams, galiojantiems teisės aktams, reglamentams ir kitiems įmonei taikomiems reikalavimams.
- Užtikrinti tinkamą įmonės informacinio turto apsaugą nuo neteisėto naudojimo, praradimo, sugadinimo ar atskleidimo.
- Užtikrinti, kad visi darbuotojai būtų supažindinti su informacijos saugumo politika ir laikytųsi jos reikalavimų.
- Nuolat tobulinti informacijos saugumo valdymo sistemą, siekiant didinti informacijos saugumo efektyvumą ir prisitaikyti prie naujų grėsmių.
- Valdyti informacijos saugumo rizikas ir taikyti tinkamas organizacines bei technines apsaugos priemones.
- Laiku nustatyti, registruoti ir valdyti informacijos saugumo incidentus bei imtis priemonių jų poveikiui mažinti, bei užkirsti kelią pasikartojimui.
- Periodiškai vertinti informacijos saugumo rizikas, siekiant nustatyti tolimesnius veiksmus ir užtikrinti tinkamą apsaugos priemonių taikymą.
- Organizuoti mokymus darbuotojams, siekiant užtikrinti informacijos saugumo ir kibernetinio saugumo praktikų taikymą kasdienėje veikloje.

**Visi darbuotojai** yra asmeniškai atsakingi už savo pareigoms priskirtų Informacijos saugumo valdymo sistemos reikalavimų supratimą, laikymąsi ir praktinį taikymą.

#### Baigiamosios nuostatos

- Visi esami ir naujai priimami darbuotojai privalo susipažinti su politika ir vykdyti jos reikalavimus.
- Su politika privalo būti supažindintos visos suinteresuotos šalys.
- Politika peržiūrima periodiškai, ne rečiau kaip kartą per metus, ir atnaujinama jei reikia.
- Politika yra skelbiama viešai, užtikrinant jos prieinamumą darbuotojams ir suinteresuotoms šalims.
- Politiką ir jos pakeitimus patvirtina įmonės direktorius.