UAB DRAUDIMO KOMPANIJA
LAMANTINAS

# Informacijos saugumo politikos santrauka

## Pagrindiniai informacijos saugumo valdymo sistemos principai

### Versijų istorija

| Versija | Data | Komentarai | Savininkas |
|---|---|---|---|
| 1.0 | 2024-04-02 | Pirma versija | I. Guzenko |
| | | | |

# 1 Bendrosios nuostatos

**UAB DK Lamantinas** (toliau - Įstaiga) pagrindinė kompanijos vykdoma veikla:

**Atsakomybės, atliekant muitinės procedūras, draudimas.**

Įstaigos vadovybė pripažįsta informacijos saugumo svarbą ir išreiškia ją įdiegdama Informacijos saugos valdymo sistema (toliau – ISVS) .

Vadovybė realizuoja informacijos saugumo valdymą, pavesdama ISVS įgyvendinimo funkciją informacijos saugumo pareigūnui. Informacijos saugumo pareigūnas organizuoja:

- Saugos priemonių įdiegimą;
- Nuolatinį Informacijos rizikos stebėjimą;
- Personalo saugos apmokymą;
- Informuoja vadovybę apie ISVS įgyvendinimo aspektus.

# 2 Įstaigos saugumo įgyvendinimo principai ir kryptys:

- užtikrinti įstaigos klientų duomenų konfidencialumą ir vientisumą, apsaugant juos nuo netinkamo atskleidimo, gavimo, laikymo, perdavimo ar sunaikinimo.
- užtikrinti draudimo paslaugų prieinamumą klientams jiems reikiamu metu ir jiems reikiama apimtimi.
- užtikrinti duomenų apsaugą saugant duomenis (eng. data protection at rest), perduodant duomenis (eng. Data protection in transit) ir tvarkant duomenis (eng. Data protection in use);
- užtikrinti nuolatinį darbuotojų kompetencijos gerinimą informacijos saugos srityje;
- užtikrinti nuolatinį gerinimą taikomų saugomų priemonių, įskaitant, bet neapsiribojant reikalavimais aprašytomis ISO27001 standarte, EU reguliavimuose ar Lietuvos teisės aktose.
- užtikrinti efektyvų paslaugų tiekėjų bei jų įgyvendinamų saugos priemonių stebėseną bei vertinimą.
- užtikrinti saugu įstaigos infrastruktūros valdymą.
- Užtikrinti organizacija pasiruošimą nenumatytoms situacijoms.