Dokumento numeris: 02
Klasifikavimas: Išoriniam naudojimui
Versija: 1
Parengė: Technologijų departamentas, IT skyrius
Galioja nuo: 2024-12-02
Paskutinės peržiūros data: 2024-12-02

Informacijos saugumo politika

Parašai

Parengė:
Technologijų departamentas, IT skyrius
Data: 2024-12-02

Patvirtino:
Lukas Kačerauskas
Data: 2024-12-02

1. Bendrosios nuostatos

Informacijos saugumo politikoje vartojamos sąvokos:

1. **ISVS** – Informacijos saugumo valdymo sistema - rizikų valdymu pagrįsta įmonės vadybos sistemos dalis, kuria siekiama sukurti, įgyvendinti, valdyti, stebėti, vertinti, prižiūrėti ir gerinti informacijos saugą.
2. **Įmonė** arba **Bendrovė**, **Organizacija** - UAB „PRODIVI" Savanorių pr. 363, LT-51480 Kaunas.
3. **Išorinės šalys** - paslaugų tiekėjai, partneriai, klientai, kiti asmenys ir organizacijos, turintys ar galintys turėti prieigą prie Įmonės informacinių išteklių.
4. **Naudotojas** - Įmonės ar Išorinės šalies darbuotojas, kuriam suteikta teisė naudotis Įmonės informaciniais ištekliais.

2. Tikslai

Organizacija įsipareigoja laikytis šių pagrindinių informacijos saugumo tikslų:

- **Konfidencialumas**: Duomenų prieigos kontrolė, prieigos teisių apribojimas ir daugiapakopio autentifikavimo naudojimas darbuotojams, klientams ir trečiosioms šalims.
- **Vientisumas**: Duomenų vientisumo palaikymas verslo analitikos sistemose, didžiųjų duomenų apdorojimo architektūrose ir užtikrinimas, kad sukurtų analitinių sprendimų veikimas būtų tikslus ir patikimas.
- **Prieinamumas**: Nepertraukiamo prieigos užtikrinimas prie duomenų ir IT paslaugų, svarbių verslo procesams.

Bendrovės ISVS siekia tokių informacijos saugumo tikslų:

- Apsaugoti prieigą prie vidinių duomenų sistemų.
- Siekti, kad grėsmių rizika neviršytų tolerancijos ribos.
- Siekti, kad darbuotojai būtų išmokyti atpažinti grėsmes ir žinotų, kaip saugiai elgtis su įmonės informacija.
- Siekti mažesnio reagavimo laiko.
- Sumažinti informacijos saugumo pažeidimų skaičių per metus.
- Pagerinti incidentų aptikimo tikslumą ir greitį.
- Padidinti darbuotojų informuotumą apie informacijos saugumą.
- Gerinti informacijos konfidencialumo, vientisumo ir prieinamumo apsaugą.
- Atitikti informacijos saugumo reikalavimus, atsižvelgiant į Bendrovės strateginius tikslus, galiojančius Europos Sąjungos ir Lietuvos Respublikos teisės aktus, taip pat Bendrovės taikomas nuostatas.

- Siekti informacijos saugumo užtikrinimo, sprendžiant pažeidimus ir šalinant jų priežastis per efektyvų incidentų valdymo procesą.
- Siekti tinkamo informacijos saugumo ir apdorojimo priemonių parinkimo ir įgyvendinimo.
- Siekti taikomų informacijos saugumo priemonių veiksmingumo.
- Siekti veiklos tęstinumo – elektroninių ryšių tinklų, informacinių procesų valdymo sistemų techninės bei programinės įrangos nepertraukiamą veiklą, incidentų valdymo ir savalaikio veiklos atstatymo.

3. Vadovybės įsipareigojimai

UAB „PRODIVI" vadovybė įsipareigoja:

- Siekti informacijos saugumo valdymo sistemos įgyvendinimą ir veiksmingumo kontrolę, ir tęstinumą.
- Suteikti būtinus išteklius politikos įgyvendinimui, įskaitant šiuolaikines technologijas.
- Kontroliuoti politikos atitiktį reikalavimams ir inicijuoti tobulinimus keičiantis darbo sąlygoms, atsirandant naujoms rizikoms ar esant reikšmingiems IT infrastruktūros pokyčiams.
- Organizacija taip pat įsipareigoja nuolat tobulinti informacijos saugumo valdymo sistemą.
- Klientams pateikti tik tokį produktą, kuris atitiktų visas saugos taisykles ir geriausią praktiką.

4. Teisės aktų laikymasis

UAB „PRODIVI" įsipareigoja laikytis galiojančių teisės aktų ir tarptautinių informacijos saugumo bei duomenų apsaugos reglamentų, įskaitant:

- Lietuvos Respublikos įstatymus, reglamentuojančius informacijos saugumą ir duomenų apsaugą.
- BDAR (Bendrasis duomenų apsaugos reglamentas).
- Vidaus reglamentus ir klientų reikalavimus, susijusius su duomenų apdorojimu, analitika ir debesų kompiuterijos sprendimais.

5. Politikos sklaida

Informacijos saugumo politika bus prieinama visiems Naudotojams ir skelbiama vidiniais komunikacijos kanalais, taip pat įmonės interneto svetainėje bei suinteresuotųjų šalių prašymu.

6. Dokumento peržiūra ir atnaujinimas

Politika bus reguliariai peržiūrima, bent kartą per metus – per vidinį auditą. Peržiūra taip pat gali būti atliekama esant technologinės infrastruktūros pokyčiams.