KVS-6-5 Informacijos saugumo politika
Galioja nuo: 2026-03-16 Leidimas: 3
Politikos rengėjas: Informacinių sistemų skyriaus vadovas
Politiką tvirtina: *Generalinis direktorius*
Publikuojama: Privačiai ☐ Viešai ☒

1 BENDROSIOS NUOSTATOS

1. Informacijos saugumo politika (toliau – Politika) yra pagrindinis dokumentas, nustatantis esminius įmonės UAB „Axioma Trade" informacijos saugumo tikslus, užtikrinimo ir valdymo principus.
2. Politika yra taikoma visiems įmonės UAB „Axioma Trade" darbuotojams, rangovams ir trečiųjų šalių tiekėjams, kurie turi prieigą prie organizacijos informacinių išteklių ir sistemų.
3. Politika parengta vadovaujantis ISO/IEC 27001:2022 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga" (toliau – ISO 27001) reikalavimais bei Europos Sąjungos TIS2 direktyvos (NIS2, 2022/2555) tinklų ir informacinių sistemų apsaugos reikalavimais, Europos Sąjungos kibernetinio atsparumo akto (CRA, 2024/2847) saugaus vystymo ir pažeidžiamumų valdymo reikalavimais.

2 INFORMACIJOS SAUGUMO VALDYMO SISTEMOS TIKSLAI

1. Apsaugoti visą informaciją nuo visų galimų grėsmių: išorinių, vidinių, tyčinių ar atsitiktinių, galinčių turėti įtakos įmonės vykdomai veiklai ir įvaizdžiui.
2. Įgyvendinti Lietuvos Respublikos teisės aktuose ir ISO 27001 standarte reglamentuotų informacijos saugumo reikalavimų laikymąsi.
3. Užtikrinti reikiamų informacijos saugumo valdymo priemonių įgyvendinimą.
4. Išvengti incidentų, susijusių su informacijos saugumo pažeidimais, galinčiais sutrikdyti įmonės veiklą, arba sumažinti tokių incidentų galimą poveikį.
5. Sukurti informacijos saugumo supratimo ir atsakomybės kultūrą visoje organizacijoje.

3 INFORMACIJOS SAUGUMO VALDYMO SISTEMA (ISVS)

ISVS padeda apsaugoti įmonės informacinius išteklius, stiprinti reputaciją ir pasiekti verslo tikslus.

3.1 Rizikos valdymas

- Rizikos vertinimas atliekamas reguliariai ir kaskart, kai organizacijoje, jos veikloje ar išorinėje aplinkoje įvyksta reikšmingų pokyčių.
- Aukščiausia vadovybė nustato rizikos priimtinumo kriterijus, reguliariai stebi rizikos vertinimą ir valdymą.

3.2 Duomenų apsauga

- Duomenys yra klasifikuojami pagal konfidencialumo kriterijus ir nustatomos jų saugos priemonės.

- Įmonė yra įsipareigojusi saugoti asmeninius ir jautrius duomenis pagal atitinkamus duomenų apsaugos reglamentus.
- Užtikrinama skaidri duomenų tvarkymo veikla ir duomenų subjektų teisės.

3.3 Turto valdymas

- Visas svarbiausias įmonės turtas yra identifikuotas, suskirstytas į kategorijas ir saugomas turto inventoriuje.
- Kiekvienam turtui priskiriami savininkai, atsakingi už jo priežiūrą ir apsaugą.

3.4 Incidentų valdymas

- Valdant informacijos saugumo incidentus yra taikomas nuoseklus ir veiksmingas incidentų valdymo procesas, sumažinantis galimą poveikį ir užtikrinantis savalaikį atkūrimą.
- Parengta reagavimo į incidentus procedūra apima klasifikavimą, prioritetų nustatymą, komunikavimą, eskalavimą bei analizę.
- Visi darbuotojai ir rangovai privalo pranešti apie pastebėtus ar įtariamus saugumo trūkumus ar incidentus.
- Išmoktos incidentų pamokos yra vertinamos, o įgyta patirtis panaudojama gerinant ISVS.
- Informacinės saugos incidentų valdymo procesai atitinka ir integruoti į Krašto apsaugos ministerijos Nacionalinio kibernetinio saugumo centro informacinės saugos incidentų valdymą.

3.5 Prieigų valdymas

- Prieiga prie informacijos ir sistemos komponentų yra leidžiama remiantis mažiausios privilegijos, "būtina žinoti" pareigybių atskyrimo principais.
- Naudotojų prieigos peržiūra atliekama periodiškai.
- Prieigos teisių suteikimo, keitimo ir atšaukimo procedūros yra dokumentuotos ir jų laikomasi.

3.6 Atsarginis kopijavimas ir atkūrimas

- Įmonės veiklai svarbių duomenų atsarginės kopijos yra daromos reguliariai.
- Atkūrimo procedūros periodiškai testuojamos, kad būtų užtikrintas greitas duomenų ir paslaugų atkūrimas gedimų atveju.

3.7 Operacijos ir ryšiai

- Siekiant užtikrinti tinkamą ir saugų informacijos apdorojimo įrenginių veikimą, veiklos procedūros ir atsakomybė yra dokumentuotos ir valdomos.
- Svarbiose sistemose įdiegta ir palaikoma apsauga nuo kenkėjiškos programinės įrangos, užtikrinami būtini atnaujinimai bei duomenų šifravimas.
- Įvykių žurnalai, kuriuose registruojami naudotojų veiksmai, išimtys, gedimai ir saugumo įvykiai rengiami, saugomi ir peržiūrimi reguliariai.

3.8 Saugus kūrimo procesas

- Įmonėje taikomas saugaus programinės įrangos kūrimo gyvavimo ciklas, kurio metu saugumas įtraukiamas į kiekvieną etapą, įskaitant statinės bei dinaminės kodo analizės priemonių naudojimą, reguliarius saugaus kodavimo praktikos mokymus.
- Atskiros kūrimo, testavimo ir gamybos aplinkos turi būti palaikomos su griežta prieigos kontrole.
- Prieš diegiant programinę įrangą turi būti atliekama išsami saugumo peržiūra.
- Užtikrinamas veiksmingas grįžtamojo ryšio mechanizmas, kad saugumo problemos, nustatytos po diegimo, būtų įtrauktos į būsimą plėtrą. Taikomas griežtas pataisų valdymas ir versijų kontrolė.

3.9 Fizinis ir aplinkos saugumas

- Nustatytos fizinio saugumo priemonės patalpoms, kuriose saugomos svarbios IT sistemos ir neskelbtina informacija ar duomenys.

3.10 Veiklos tęstinumo ir atkūrimo planavimas

- Įmonė turi veiklos tęstinumo ir atkūrimo planą, kuriame atsižvelgta į galimas grėsmes bei veiklos sutrikimus.
- Šis planas yra testuojamas ir peržiūrimas reguliariai, kad būtų užtikrintas jo veiksmingumas ekstremalių situacijų atveju.

3.11 Santykiai su tiekėjais

- Informacijos saugumo reikalavimai tiekėjams, turintiems prieigą prie bendrovės informacinių sistemų ir turto, nurodomi sutartyse.
- Tiekėjų atitiktis informacijos saugumo reikalavimams yra vertinama periodiškai.

3.12 Darbuotojų mokymas

- Darbuotojai reguliariai mokomi apie informacijos saugumą ir duomenų apsaugą.
- Specialūs mokymai rengiami asmenims atliekantiems konkrečias saugumo funkcijas ir prisiimantiems atsakomybę.

3.13 Nuolatinis tobulėjimas

- ISVS tinkamumas ir efektyvumas yra tobulinamas atliekant rizikos vertinimą, veiksmingumo matavimą, vidaus auditą, ISVS vadybos vertinamąją analizę, numatant ir įgyvendinant korekcinius veiksmus.

4 GALIOJIMAS IR DOKUMENTŲ VALDYMAS

1. Informacijos saugumo politika peržiūrima ne rečiau kaip kartą per metus arba po bet kokio reikšmingo saugumo incidento, reguliavimo pakeitimų ar organizacinių pokyčių.
2. Informacijos saugumo politika yra prieinama visoms suinteresuotosioms šalims.
3. Su Politika ir jos pakeitimais visi darbuotojai supažindinami per dokumentų valdymo sistemą (DVS) arba kitomis priemonėmis.

Leidimo Nr.	Parengimo data	Leidimo aprašymas	Leidimo priežastis	Leidimą parengė (padalinys)
1.	2023-11-20	Išleistas dokumentas	Naujas	Kokybės skyrius
2.	2024-03-14	Išleistas dokumentas	Politikos nuostatos (p.3,4,5,6) perkeltos į Informacijos saugumo valdymo tvarką	Kokybės skyrius
3.	2026-03-16	Dokumento papildymai	Atitikties ES direktyvoms TIS2 ir CRA deklaravmas	Informacinių sistemų skyrius