PATVIRTINTA
UAB „Toksika“ valdybos
2025 m. spalio 29 d. sprendimu,
posėdžio protokolas Nr. 339

UAB „TOKSIKA“ TINKLŲ IR INFORMACINIŲ SISTEMŲ KIBERNETINIO SAUGUMO POLITIKA

1. BENDROSIOS NUOSTATOS

1.1. UAB „Toksika“ (toliau – Bendrovė) tinklų ir informacinių sistemų kibernetinio saugumo politika (toliau – Politika) apibrėžia Bendrovės veiklos, susijusios su tinklų ir informacinių sistemų apsauga, organizavimo tvarką, bendruosius kibernetinio saugumo reikalavimus ir įpareigojimus, kurių turi laikytis Bendrovės vadovas, visi darbuotojai, valdybos nariai bei trečiosios šalys, taip pat nurodo teisės aktus ir kitus dokumentus, kuriais vadovaujamasi įgyvendinant Politiką.

1.2. Politikoje vartojamos sąvokos suprantamos taip, kaip jos apibrėžtos Lietuvos Respublikos kibernetinio saugumo įstatyme, Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatyme, Lietuvos standartuose LST EN ISO/IEC 27001 ir LST EN ISO/IEC 27002 ir kituose teisės aktuose, reglamentuojančiuose informacijos saugumo valdymą, saugų tinklų ir informacinių sistemų ir (ar) informacinių išteklių naudojimą.

1.3. Kitos Politikoje vartojamos sąvokos ir sutrumpinimai:

1.3.1. Bendrovės vadovas – Bendrovės generalinis direktorius;

1.3.2. Bendrovės vadovybė – pareigybės, kurios pagal valdybos patvirtintą Bendrovės organizacinę struktūrą atitinka lygmenis „aukščiausiojo lygmens vadovai“ ir „viduriniojo lygmens vadovai“.

1.3.3. kibernetinio saugumo vadovas – viešojo pirkimo būdu atrinktas paslaugų teikėjas, kuris pagal Lietuvos Respublikos kibernetinio saugumo įstatymo 15 straipsnį atlieka Bendrovės kibernetinio saugumo vadovo ir saugos įgaliotinio funkcijas;

1.3.4. trečioji šalis – asmuo (bet kuris juridinis asmuo arba fizinis asmuo, kuris nėra Bendrovės darbuotojas ar valdybos narys), turintis atitinkamus teisinius santykius su Bendrove ir dėl to galintis turėti prieigą prie Bendrovės informacinių išteklių.

1.4. Politikos tikslas – nustatyti Bendrovės tinklų ir informacinių sistemų kibernetinio saugumo principus ir valdymo kryptis, siekiant užtikrinti duomenų ir informacijos konfidencialumą, vientisumą bei prieinamumą, veiklos tęstinumą ir teisės aktų nustatytų kibernetinio saugumo reikalavimų įgyvendinimą.

1.5. Politikos ir ją įgyvendinančių dokumentų nuostatos yra taikomos Bendrovės vadovui, visiems darbuotojams, valdybos nariams ir trečiosioms šalims.

2. VEIKLOS UŽTIKRINANT KIBERNETINĮ SAUGUMĄ TIKSLAI IR PRIORITETINĖS KRYPTYS

2.1. Bendrovės veiklos užtikrinant kibernetinį saugumą tikslai yra:

2.1.1. užtikrinti Bendrovės tinklų ir informacinių sistemų patikimą bei saugų veikimą, įskaitant duomenų ir informacijos konfidencialumą, vientisumą ir prieinamumą.

2.1.2. įgyvendinti nuoseklų kibernetinio saugumo rizikų, pokyčių, spragų ir pataisų valdymą, užtikrinant technologinių sprendimų atitiktį saugumo reikalavimams bei licencijuotos, patikrintos programinės įrangos naudojimą.

2.1.3. užtikrinti kibernetinių incidentų prevenciją, aptikimą, valdymą ir veiklos tęstinumą galimų incidentų atveju.

2.1.4. ugdyti vadovybės ir darbuotojų atsakomybę bei kompetencijas kibernetinio saugumo srityje, organizuojant mokymus ir diegiant kibernetinės higienos principus.

2.2. Tinklų ir informacinių sistemų duomenų ir elektroninės informacijos kibernetinio saugumo užtikrinimo prioritetinės kryptys:

2.2.1. duomenų ir elektroninės informacijos konfidencialumo, vientisumo ir prieinamumo užtikrinimas;

2.2.2. duomenų ir elektroninės informacijos tvarkymo kontrolė;

2.2.3. duomenų ir elektroninės informacijos tvarkymui naudojamos techninės ir programinės įrangos kontrolė;

2.2.4. tvarkomų asmens duomenų apsauga.

3. KIBERNETINĮ SAUGUMĄ REGLAMENTUOJANTYS TEISĖS AKTAI

3.1. Teisės aktai, kuriais vadovaujantis tvarkomas ir užtikrinamas Bendrovės tinklų ir informacinių sistemų kibernetinis saugumas:

3.1.1. Lietuvos Respublikos kibernetinio saugumo įstatymas;

3.1.2. Lietuvos Respublikos valstybės informacinių išteklių valdymo įstatymas;

3.1.3. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas;

3.1.4. 2016 m. balandžio 27 d. Europos Parlamento ir Tarybos reglamentas (ES) 2016/679 dėl fizinių asmenų apsaugos tvarkant asmens duomenis ir dėl laisvo tokių duomenų judėjimo ir kuriuo panaikinama Direktyva 95/46/EB (Bendrasis duomenų apsaugos reglamentas);

3.1.5. Kibernetinio saugumo reikalavimų aprašas, patvirtintas Lietuvos Respublikos Vyriausybės 2018 m. rugpjūčio 13 d. nutarimu Nr. 818 „Dėl Lietuvos Respublikos kibernetinio saugumo įstatymo įgyvendinimo“;

3.1.6. Informacinių technologijų saugos atitikties vertinimo metodika, patvirtinta Lietuvos Respublikos krašto apsaugos ministro 2020 m. gruodžio 4 d. įsakymu Nr. V-941 „Dėl Informacinių technologijų saugos atitikties vertinimo metodikos patvirtinimo“;

3.1.7. Lietuvos standartai LST EN ISO/IEC 27001 ir LST EN ISO/IEC 27002 bei kiti Lietuvos ir tarptautiniai standartai, reglamentuojantys informacijos saugą;

3.1.8. kiti teisės aktai, reglamentuojantys duomenų ir elektroninės informacijos kibernetinio saugumo valdymą, saugų tinklų ir informacinių sistemų ir (ar) informacinių išteklių naudojimą.

4. DOKUMENTAI, KURIAIS VADOVAUJAMASI ĮGYVENDINANT POLITIKĄ

4.1. Politikai įgyvendinti Bendrovės vadovas savo įsakymais nustato organizacines ir technines kibernetinio saugumo užtikrinimo priemones (tvarkas, procedūras, taisykles), reguliuojančias šias sritis:

4.1.1. tinklų ir informacinių sistemų rizikos vertinimo ir valdymo tvarką;

4.1.2. kibernetinių incidentų valdymo, žurnalinių įrašų (angl. log) administravimo ir saugojimo, įsibrovimų aptikimo ir prevencijos tvarką;

4.1.3. tinklų ir informacinių sistemų veiklos tęstinumo valdymo ir veiklos atkūrimo planavimą, veiklos tęstinumo valdymo plano veiksmingumo išbandymo ir ataskaitų rengimą, atsarginių duomenų kopijų kūrimo, saugojimo ir duomenų atkūrimo iš jų tvarką;

4.1.4. tiekimo grandinės saugumo valdymo tvarką;

4.1.5. tinklų ir informacinių sistemų įsigijimo, plėtojimo ir priežiūros saugumo užtikrinimo tvarką, spragų (pažeidžiamumų) valdymo ir atskleidimo procedūras;

4.1.6. kibernetinio saugumo reikalavimų veiksmingumo vertinimo tvarką;

4.1.7. kibernetinės higienos praktikos organizavimo ir kibernetinio saugumo mokymų organizavimo ir vykdymo tvarką;

4.1.8. kriptografijos ir šifravimo naudojimo tvarką;

4.1.9. žmogiškųjų išteklių saugumo, tinklų ir informacinių sistemų fizinės prieigos reikalavimus, turto valdymo tvarką;

4.1.10. prieigos valdymo tvarką.

5. ATSAKOMYBĖ UŽ POLITIKOS ĮGYVENDINIMĄ

5.1. Bendrovės vadovas, visi darbuotojai, valdybos nariai ir trečiosios šalys pagal kompetenciją atsako už tinklų ir informacinių sistemų, jose tvarkomų duomenų ir kito Bendrovės turto kibernetinį saugumą.

5.2. Bendrovės valdyba atsakinga už Politikos tvirtinimą ir keitimą bei valdybos kompetencijai pagal įstatus priskiriamus sprendimus, būtinus kibernetinio saugumo vadovo funkcijai Bendrovėje užtikrinti.

5.3. Bendrovės vadovas atsakingas už kibernetinio saugumo vadovo funkcijos Bendrovėje užtikrinimą (įskaitant paslaugų sutarties sudarymą bei funkcijų ir atsakomybės nustatymą), Politiką įgyvendinančių dokumentų tvirtinimą ir keitimą, būtinų išteklių (techninių, finansinių ir kitų) Politikai įgyvendinti skyrimą, visų darbuotojų ir valdybos narių supažindinimą su Politikos nuostatomis bei atsakomybės už Politikos reikalavimų nesilaikymą reglamentavimą ir taikymą.

5.4. Bendrovės strategijos ir finansų vadovas atsakingas už Politikos įgyvendinimo priemonių ir išteklių numatymą Bendrovės strateginiame veiklos plane ir metiniuose planavimo dokumentuose.

5.5. Bendrovės plėtros vadovas atsakingas už kibernetinio saugumo vadovo ir Bendrovės struktūrinių padalinių vadovų darbo, įgyvendinant Politiką, koordinavimą, su kibernetiniu saugumų susijusių rizikų įtraukimą į Bendrovės rizikų registrą ir jų stebėseną bei savalaikį Politikos teikimą valdybai peržiūrėti.

5.6. Kibernetinio saugumo vadovo funkcijų ir atsakomybės aprašymą tvirtina Bendrovės vadovas. Be kitų atsakomybių, kibernetinio saugumo vadovas atsakintas už Politikos ir ją įgyvendinančių dokumentų nuostatų atitiktį Lietuvos Respublikos teisės aktams ir Bendrovės veiklos specifikai bei Politikos ir ją įgyvendinančių dokumentų parengimą ir jų keitimo inicijavimą.

5.7. Bendrovės vadovybė užtikrina, kad:

5.7.1. visi darbuotojai, valdybos nariai ir trečiosios šalys būtų susipažindintos su Politika;

5.7.2. prieiga prie Bendrovės tinklų ir informacinių sistemų būtų suteikiama tik susipažinus su Politika ir ją įgyvendinančiais dokumentais bei įsipareigojus jų laikytis;

5.7.3. Politika ir ją įgyvendinantys dokumentai trečiosioms šalims teikiami susipažinti tiek, kiek būtina jų funkcijoms vykdyti, laikantis konfidencialumo ir principo „būtina žinoti“.

5.8. Bendrovės vadovas, darbuotojai, valdybos nariai ir trečiosios šalys, pažeidę Politikos, ją įgyvendinančių dokumentų ar kitų su kibernetinio saugumo užtikrinimu susijusių teisės aktų nuostatas, atsako Lietuvos Respublikos ir Bendrovės vidaus teisės aktų nustatyta tvarka.

6. BAIGIAMOSIOS NUOSTATOS

6.1. Politika tvirtinama ir keičiama valdybos sprendimu. Ji peržiūrima ne rečiau kaip vieną kartą per metus, esant poreikiui Politika koreguojama, siekiant užtikrinti jos nuostatų atitiktį Lietuvos Respublikos teisės aktams ir aktualumą.

6.2. Politika ir ją įgyvendinantys dokumentai atnaujinami, atsižvelgiant į rizikos vertinimo rezultatus, teisės aktų pakeitimus, institucijų rekomendacijas, gerąją praktiką, trečiųjų šalių pastabas, auditų ir stebėsenos išvadas bei įvykusius incidentus.

6.3. Bendrovė per 5 darbo dienas nuo Politikos ar ją įgyvendinančių dokumentų patvirtinimo / pakeitimo pateikia ar atnaujina jų duomenis (pavadinimą, patvirtinimo datą ir registracijos numerį) Nacionaliniam kibernetinio saugumo centrui per Kibernetinio saugumo informacinę sistemą (KSIS).

6.4. Politika nėra skelbiama Bendrovės interneto tinklalapyje, tačiau trečiosioms šalims sudaroma galimybė su ja susipažinti laikantis Politikos 5.7.3 punkto sąlygų ir pasirašius konfidencialumo susitarimą.