crowdpear

Verslo centras ELEVEN
Kareivių g.11B
LT-09109 Vilnius, Lietuva

Crowdpear, UAB
+370 615 54424
info@crowdpear.com

Versija galioja nuo: 2025-08-12

INFORMACIJOS SAUGUMO POLITIKA

1. TIKSLAS

1.1. Ši UAB „Crowdpear“ informacijos saugumo politika (toliau – Politika) nustato UAB „Crowdpear“ (toliau - Bendrovė) informacinių ir ryšių technologijų (toliau – IRT) turto apsaugos sistemą. Politika siekiama įgyvendinti, palaikyti ir nuolat tobulinti informacijos saugumą Bendrovėje. Ši politika yra pagrindinis dokumentas, apibrėžiantis informacijos saugumo valdymą ir sudarantis visų informacijos saugumo procedūrų ir standartų pagrindą.

2. TAIKYMO SRITIS

2.1. Ši Politika taikoma valdant ir naudojant visą Bendrovės informacinių ir ryšių technologijų turtą (toliau – IRT turtas), nepriklausomai nuo turto vietos ar formato, įskaitant bet neapsiribojant visas informacines sistemas, programas, infrastruktūrą, verslo procesus ir fizines patalpas, susijusias su informacijos tvarkymu, saugojimu ir perdavimu. Politika privalo vadovautis visi darbuotojai, rangovai, konsultantai, laikinieji darbuotojai ir trečiųjų šalių subjektai, kurie turi prieigą prie Bendrovės IRT turto arba yra už jį atsakingi.

3. BENDROSIOS NUOSTATOS

3.1. Politikoje atsižvelgiama į dabartinę informacinių technologijų plėtros Bendrovėje padėtį ir ateities perspektyvas, jų veikimo tikslus ir uždavinius, veikimo režimus, taip pat pateikiamas grėsmių Bendrovės informacinių ryšių objektų ir subjektų saugumui sąrašas.

3.2. Visos šioje Politikoje vartojamos sąvokos ir santrumpos yra nurodytos UAB *„Crowdpear“ atitikimo DORA ir ISO 27001 terminų vadove“.*

3.3. Šios Politikos reikalavimai taikomi visiems Bendrovės struktūriniams padaliniams.

3.4. Politika yra pagrindas:

1) Vieningos informacijos saugumo užtikrinimo Bendrovėje politikos sukūrimui ir palaikymui;
2) Saugomos informacijos identifikavimo organizavimo, jos konfidencialumo lygio pagrindimui ir dokumentavimui atitinkamuose sąrašuose;
3) Valdymo sprendimų priėmimui ir praktinių priemonių, skirtų informacinių sistemų saugumo politikai įgyvendinti, kūrimui.
4) Suderintų priemonių rinkinio, skirto įvairių tipų informacijos saugumo grėsmių identifikavimui, neutralizavimui ir pasekmių šalinimui, sukūrimui.
5) Bendrovės struktūrinių padalinių veiklos koordinavimui kuriant, tobulinant ir eksploatuojant informacines technologijas, užtikrinant informacijos saugumo reikalavimų laikymąsi.
6) Pasiūlymų dėl teisinių, reguliavimo, techninių ir organizacinių sistemų, skirtų užtikrinti informacijos saugumą Bendrovėje, tobulinimo rengimui.

3.5. Informacinių išteklių apsauga vykdoma pagal Informacijos saugumo valdymo sistemą (toliau – ISVS), kuri atitinka:

- Tarptautinio informacijos saugumo standarto ISO/IEC 27001:2022 reikalavimus.
- DORA (Skaitmeninio operacinio atsparumo įstatymo) reglamento (ES) 2022/2554 reikalavimus, užtikrinančius IRT sistemų ir procesų atsparumą, saugumą ir vientisumą.
- Bendrovės teisės aktų, norminių ir sutartinių įsipareigojimų reikalavimus dėl informacijos saugumo.
- Šią Bendrovės *Politiką*.

3.6. Bendrovės Informacijos saugumo valdymo sistema (ISVS) taikymo sritis apima sėkmingą programinės įrangos kūrimo paslaugų teikimą, palaikymą ir priežiūrą (žr. dokumentą *„Pareiškimas dėl tinkamumo“*).

3.7. Bendrovės vadovas yra atsakingas už informacijos saugumo užtikrinimą Bendrovėje. Darbuotojai privalo būti tinkamai supažindinti su ISVS dokumentais ir laikytis juose nustatytų reikalavimų.

3.8. Ši Politika reguliariai peržiūrima bent kartą per dvejus metus.

3.9. Politika siekiama šių tikslų:

1) Naudojamos ir tvarkomos informacijos vientisumo apsauga;
2) Kritinės informacijos konfidencialumo išlaikymas, kaip apibrėžta Informacinių ir ryšių technologijų turto valdymo politikoje.
3) Bendrovės informacinėse sistemose tvarkomos informacijos prieinamumo užtikrinimas.
4) Pagrindinių verslo procesų tęstinumo užtikrinimas.

3.10. Siekiant šių tikslų, reikia įgyvendinti žemiau išvardintas užduotis:
1) Užtikrinti aktyvų vadovybės įsitraukimą į Bendrovės informacijos saugumo valdymą;
2) Didinti darbuotojų informuotumą apie su informacijos ištekliais susijusias rizikas;
3) Aiškiai paskirstyti darbuotojams atsakomybes ir pareigas siekiant užtikrinti informacijos saugumą;
4) Įdiegti darbuotojų prieigų prie Bendrovės techninės įrangos saugyklos, programinės įrangos ir informacinių išteklių kontrolę;
5) Registruoti vartotojų veiksmus sistemos žurnaluose, kai naudojami tinklo ištekliai;
6) Apsaugoti informacinės saugumo veikimo procesą nuo išorės įsikišimo;
7) Kontroliuoti programinės įrangos priemonių ir jų vykdymo aplinkos vientisumą, atkurti ją sutrikimo atveju ir apsaugoti sistemas nuo kenkėjiškų kodų įvedimo;
8) Apsaugoti ribojamą informaciją ir asmens duomenis nuo nutekėjimo techniniais kanalais juos apdorojant, saugant ir perduodant ryšio kanalais;
9) Užtikrinti vartotojų autentifikavimą informacijos saugumo srityje ir prieigoje prie išteklių;
10) Laiku nustatyti informacijos saugumo grėsmes, taip pat priežastis ir sąlygas, kurios prisideda prie žalos atsiradimo;
11) Sukurti sąlygas, kad būtų galima sumažinti ir lokalizuoti žalą, padarytą dėl neteisėtų asmenų ar organizacijų veiksmų;
12) Taikyti teisės aktuose ar vidiniuose teisės aktuose numatytą atsakomybę informacijos saugumo politikos pažeidimų atveju;
13) Šalinti informacijos saugumo pažeidimų padarinius;
14) Kurti ir įgyvendinti informacijos saugumo užtikrinimo taisykles ir instrukcijas, taip pat stebėti, kaip Bendrovės darbuotojai jų laikosi;
15) Įgyvendinti informacijos rizikos vertinimo, valdymo ir sumažinimo priemones (žr. dokumentus: *„Informacinių ir ryšių technologijų rizikos vertinimo metodika“, „Reagavimo į incidentus planas“, „Asmens duomenų saugumo pažeidimų valdymo politika“);*
16) Nuolat tobulinti ISVS.

4. ATSAKOMYBĖS IR ĮSIPAREIGOJIMAI

4.1. Vadovybė tiesiogiai dalyvauja sprendžiant su informacijos saugumu susijusius klausimus pagal Bendrovės (verslo) tikslus, įstatymus ir kitus teisės aktus.

4.2. Vadovybė palaiko nustatytą informacijos saugumo lygį įdiegdama ISVS ir paskirdama darbuotojams atsakomybę bei pareigas už jos priežiūrą.

4.3. Informacijos saugumo pareigūnas:
1) Formuluoja, peržiūri ir rengia Informacijos saugumo politiką bei stebi jos įgyvendinimo efektyvumą;
2) Užtikrina aiškų valdymą ir aktyvų palaikymą informacijos saugumo iniciatyvoms;
3) Užtikrina, kad informacijos saugumo programai būtų skirta pakankamai išteklių;
4) Koordinuoja informacijos saugumo kontrolės priemones visoje Bendrovėje;
5) Tvirtina su informacijos saugumu susijusias darbuotojų funkcijas ir pareigas, pateikdamas pareigybių aprašymus, įsakymų projektus ir kt.;
6) Tvirtina pasirengimo lygį ir su informacijos saugumu susijusią rizikos toleranciją organizacijoje;
7) Inicijuoja planus ir programas, skirtas didinti informacijos saugumo informuotumą, nustato vartotojų ir administratorių mokymo saugumo metodų ir procedūrų srityje poreikį ir nustato atsakomybę už programinės ir aparatinės įrangos diegimą ir priežiūrą;
8) Nustato vidinių ar išorinių specialistų konsultacijų informacijos saugumo klausimais poreikį ir stebi rekomendacijų įgyvendinimą visoje Bendrovėje;
9) Aiškiai nustato skyrių vadovų atsakomybę už įvairų turtą ir saugumo procesus. Išsami informacija apie šias pareigas yra dokumentuota, o valdžios lygiai yra aiškiai apibrėžti ir dokumentuoti (žr. Materialinės atsakomybės sutartį).
10) Inicijuoja tyrimus dėl informacijos saugumo politikos pažeidimų;
11) Pašalina informacijos saugumo pažeidimų pasekmes;
12) Laiku nustato ir užkerta kelią bandymams pažeisti nustatytas informacijos saugumo taisykles.

4.4. Siekdama būti informuota apie besikeičiančias kibernetinio saugumo grėsmes, reguliavimo pokyčius ir geriausią pramonės praktiką, Bendrovė aktyviai bendradarbiauja su atitinkamomis profesinėmis bendruomenėmis, pramonės grupėmis ir kibernetinio saugumo asociacijomis. Informacijos saugumo pareigūnas yra atsakingas už tokios sąveikos priežiūrą ir pagrindinių įžvalgų bei rekomendacijų integravimą į informacijos saugumo valdymo sistemą (ISVS).

4.5. Vartotojo veiklos, kiekvienos saugos priemonės ir bet kurio apsaugos objekto kontrolė vykdoma naudojant operatyvinio valdymo ir registravimo įrankius (žr. dokumentą „Prieigos kontrolės politika“). Ši kontrolė apima tiek neteisėtus, tiek teisėtus vartotojų veiksmus.

4.6. Darbuotojai yra informuojami apie savo pareigas saugoti informaciją pagal savo darbo funkcijas, taip pat apie galimų pažeidimų pasekmes. Informacijos saugumo pareigūnas atsako už šios informacijos

teikimą ir užtikrinimą, kad darbuotojai būtų tinkamai supažindinti su saugumo reikalavimais, susijusiais su jų darbo funkcijomis.

4.7. Infrastruktūros administratoriai prisiima administracinę ir kitą atsakomybę už informacijos saugumo politikos pažeidimus pagal galiojančius įstatymus. Infrastruktūros administratorių pareigos apibrėžtos *„Infrastruktūros administratoriaus vadove“*. Infrastruktūros administratoriai užtikrina nepertraukiamą tinklo veikimą ir yra atsakingi už techninių priemonių, būtinų Informacijos saugumo politikai vykdyti, įgyvendinimą.

5. PAGRINDINIAI INFORMACIJOS SAUGUMO UŽTIKRINIMO PRINCIPAI

5.1. Pagrindiniai Bendrovės informacijos saugumo užtikrinimo principai:

1) Teisinių reikalavimų laikymasis – galiojančių įstatymų ir kitų norminių aktų laikymasis.
2) Atitiktis tarptautiniams ir nacionaliniams standartams – šalyje galiojančių informacijos saugumo standartų laikymosi užtikrinimas.
3) Nuolatinė informacinės aplinkos analizė – IRT turto pažeidžiamumų nustatymas.
4) Priežasties ir pasekmės ryšių nustatymas - potencialių problemų supratimas ir tiksli jų raidos prognozė.
5) Nustatytų problemų poveikių vertinimas.
6) Visapusiškas apsaugos metodų naudojimas - fizinių, organizacinių, technologinių ir teisinių priemonių taikymas kompiuterinėms sistemoms apsaugoti, apimant visus svarbius grėsmės kanalus be silpnų vietų komponentų sandūrose. Apsaugos priemonės neturi trukdyti siekti įstatymų nustatytų tikslų ar apsunkinti informacijos apdorojimo.
7) Efektyvus apsaugos priemonių įgyvendinimas.
8) Apsaugos priemonių lankstumas - informacijos saugumo priemonių pritaikymas prie kintančių išorinių sąlygų ir reikalavimų laikui bėgant.
9) Nuolatinis informacijos saugumo priemonių tobulinimas - organizacinių ir techninių pasiekimų naudojimas, informacijos saugumo efektyvumo analizė, šiuolaikinių informacijos perėmimo ir apsaugos metodų diegimas, norminių teisės aktų reikalavimų laikymasis ir geriausios šalies ir tarptautinių organizacijų praktikos įgyvendinimas.
10) Saugios veiklos tęstinumas - nepertraukiamo informacijos saugumo principų laikymosi užtikrinimas.
11) Savalaikis pažeidimų aptikimas ir prevencija - aktyviai aptikti ir pašalinti nustatytų informacijos saugumo taisyklių pažeidimus.
12) Aiškus informacijos saugumo tikslų apibrėžimas - pašalinti neaiškumus, susijusius su organizacine struktūra, darbuotojų funkcijomis, politika, ir įvertinti saugumo priemonių tinkamumą, dokumentuojant funkcinius ir saugumo tikslus.
13) Atsakomybė už informacijos saugumą - asmeninės atsakomybės už informacijos saugumą ir informacijos apdorojimo sistemas priskyrimas kiekvienam darbuotojui pagal jo įgaliojimus. Teisių ir pareigų paskirstymas užtikrina, kad pažeidimo atveju atsakinga šalis būtų aiškiai nustatyta.
14) Paslaugų prieinamumas - paslaugų ir sistemų prieinamumo klientams ir partneriams užtikrinimas per susitarimuose, sutartyse ir kituose dokumentuose nustatytus terminus.
15) Informacijos saugumo stebėjimas ir vertinimas - užtikrinamas skaidrumas ir leidžiama įgaliotiems specialistams įvertinti apsaugos priemonių veiksmingumą.
16) Informacijos klasifikavimas - apdorotos informacijos kategorizavimas ir jos svarbos lygio nustatymas pagal teisės aktus.

6. PERSONALO POLITIKA SKIRTA INFORMACIJOS SAUGUMO UŽTIKRINIMUI

6.1. Darbuotojų pareigos ir atsakomybė yra aiškiai apibrėžtos bendrovės vidaus teisės aktuose.

6.2. Darbuotojai pasirašo darbo sutartis, kuriose išdėstytos pagrindinės pareigos, susijusios su informacijos saugumu. Konkrečios informacijos saugumo pareigos yra apibrėžtos vidaus politikoje ir taisyklėse, su kuriomis darbuotojus privalo supažindinti informacijos saugumo pareigūnas.

6.3. Darbuotojai ir trečiųjų šalių organizacijų atstovai, naudojantys Bendrovės informacijos apdorojimo priemones, pasirašo sutartis, atitinkančias informacijos saugumo reikalavimus, siekiant sumažinti vagystės, sukčiavimo, įrangos netinkamo naudojimo ir informacijos saugumo grėsmių riziką.

6.4. Prieš suteikiant prieigą prie informacijos apdorojimo priemonių, darbuotojai, rangovai ar išoriniai naudotojai pasirašo konfidencialumo sutartį (KS).

6.5. Visi kandidatai, pretenduojantys į nuolatinį darbą, patikrinami pagal galiojančius teisės aktus, užtikrinant asmens duomenų konfidencialumą. Tikrinama ši kandidatų pateikta informacija:

1) Ankstesnių darbdavių rekomendacijos, jei yra ir jeigu kandidatas sutiko.
2) Kandidato gyvenimo aprašymas.
3) Išsilavinimo ir profesinės kvalifikacijos dokumentai.
4) Asmens tapatybės dokumentai.

5) Kita informacija, kurią reikia patikslinti.

6.6. Informacija apie visus į nuolatines pareigas priimtus darbuotojus renkama ir tvarkoma laikantis BDAR, įstatymų ir Bendrovės vidaus politikos bei taisyklių dėl duomenų rinkimo, saugojimo, naudojimo ir apsaugos, kaip nurodyta atitinkamuose UAB „Crowdpear“ dokumentuose.

6.7. Informacijos saugumo specialistas informuoja darbuotojus apie šios Politikos reikalavimus ir visą su informacijos saugumu susijusią dokumentaciją, siekdamas didinti informuotumą, apmokyti juos apie reagavimo į incidentus tvarką ir užkirsti kelią galimiems pažeidimams. Yra taikomos priemonės, užtikrinančios, kad pasibaigus darbuotojų darbo santykiams būtų grąžintas visas jų naudotas IRT turtas (pvz., kompiuterinė įranga, oficialūs dokumentai, elektroninės laikmenos). Tais atvejais, kai naudojama asmeninė įranga, darbuotojai privalo perduoti informaciją atitinkamo skyriaus vadovui (arba atsakingam specialistui) arba perduoti ją ištrinti Informacijos saugumo pareigūnui naudojant metodus, kurie neleidžia jos atkurti (žr. dokumentus „IRT turto valdymo politika“ ir „Prieigos kontrolės politika“). Informacijos ištrynimo procesas turi būti patikrintas ir užfiksuotas oficialiu susitarimu.

6.8. Prieigos teisės prie informacinių sistemų ir išteklių panaikinamos nutraukus darbuotojo darbo sutartį arba peržiūrimos pasikeitus jo pareigoms ar funkcijoms.

6.9. Darbuotojų paskyros deaktyvuojamos nutraukus darbo sutartį dėl ilgalaikių komandiruočių, atostogų (ilgiau nei 60 dienų) arba pasibaigus darbo sutarčiai.

7. IŠORINIS APSIKEITIMAS INFORMACIJA

7.1. Išorinis apsikeitimas informacija su organizacijos klientais, tiekėjais ir kitais suinteresuotaisiais asmenimis vykdomas per kurjerių tarnybas, paštą ir (arba) el. paštą, taip pat elektronines dokumentų valdymo sistemas, jei šiuos metodus už informacijos saugumą atsakingas asmuo laiko priimtinais keistis informacija pagal Bendrovės informacijos saugumo politiką ir norminius reikalavimus.

7.2. Informacija apie saugumą santykiuose su tiekėjais aptariama sutartyse su tiekėjais. Šiose sutartyse nurodomi informacijos saugumo reikalavimai, siekiant sumažinti riziką, susijusią su tiekėjų prieiga prie Bendrovės IRT išteklių, įskaitant apdorojimo, saugojimo, perdavimo ir sąveikos procesus, taip pat IT infrastruktūros komponentų teikimą. Jose taip pat apibrėžiamos priemonės, skirtos spręsti informacijos saugumo rizikas, susijusias su informacinių ir ryšių technologijų paslaugomis ir produktų tiekimo grandine.

8. PAREIŠKIMAI DĖL INFORMACIJOS SAUGUMO POLITIKOS

8.1. Rizikos valdymas

8.1.1. Bendrovė diegia ir palaiko visapusišką rizikos valdymo sistemą, kuri identifikuoja, įvertina ir apdoroja informacijos saugumo rizikas pagal verslo tikslus ir suinteresuotųjų šalių reikalavimus.

8.1.2. Rizikos vertinimai atliekami numatytais intervalais, ne rečiau kaip kartą per metus, ir kai įvyksta reikšmingų verslo aplinkos, technologinės infrastruktūros ar grėsmių aplinkos pokyčių.

8.1.3. Rizikos vertinimo metodikoje atsižvelgiama tiek į grėsmes, tiek į pažeidžiamumus, įvertinamas galimas poveikis informacijos konfidencialumui, vientisumui, autentiškumui ir prieinamumui bei dokumentuojamas rizikos valdymo sprendimų pagrįstumas.

8.1.4. Rizikos valdymo planai rengiami ir įgyvendinami remiantis organizacijos nustatytais rizikos priėmimo kriterijais, reguliariai stebint rizikos valdymo veiksmingumą ir teikiant ataskaitas atitinkamiems suinteresuotiesiems subjektams.

8.2. Prieigos kontrolės valdymas

8.2.1. Bendrovė diegia ir palaiko visapusišką prieigos kontrolės sistemą, pagrįstą minimalių privilegijų ir „būtinybės žinoti“ principais.

8.2.2. Visa prieiga prie informacinių sistemų ir duomenų kontroliuojama taikant formalias vartotojų registracijos ir išregistravimo procedūras.

8.2.3. Prieigos teisės suteikiamos tik gavus dokumentuotą išteklių savininko ir informacijos saugumo komandos patvirtinimą.

8.2.4. Daugialypė autentifikacija yra privaloma visų tipų nuotolinei prieigai ir prieigai prie privilegijuotų paskyrų.

8.2.5. Reguliarios prieigos peržiūros atliekamos ne rečiau kaip kas ketvirtį, o prieigos teisės nedelsiant panaikinamos nutraukus darbo sutartį ar pasikeitus pareigoms.

8.2.6. Bendrovė tvarko visų prieigos kontrolės pakeitimų audito žurnalus su automatiniais įspėjimais apie įtartinus prisijungimo bandymus ar neteisėtą piktnaudžiavimą privilegijomis.

8.2.7. Slaptažodžių politika užtikrina griežtus autentifikavimo reikalavimus, įskaitant minimalų ilgį, sudėtingumą ir reguliarų slaptažodžių keitimą, taip pat technines kontrolės priemones, skirtas užkirsti kelią slaptažodžių pakartotiniam naudojimui.

8.3. IRT turto valdymas ir klasifikavimas

8.3.1. Bendrovė tvarko visapusišką visų IRT išteklių, įskaitant fizinius ir loginius, inventorių, aiškiai nurodydama savininkus ir apibrėžtas saugumo atsakomybes, kaip nurodyta *IRT turto valdymo politikoje.* Informacijos saugumo pareigūnas yra atsakingas už IRT išteklių klasifikavimą ir saugumo reikalavimų laikymosi užtikrinimą, o IT pagalbos tarnyba tvarko inventorių ir užtikrina gyvavimo ciklo valdymą.

8.3.2. Visi IRT ištekliai klasifikuojami pagal jų jautrumą, kritiškumą ir teisinius reikalavimus, naudojant Bendrovės nustatytą klasifikavimo schemą. IRT išteklių savininkai atsako už tai, kad būtų užtikrintos tinkamos tvarkymo procedūros, atsižvelgiant į turto klasifikavimo lygį.

8.3.3. Turto inventorius peržiūrimas ir atnaujinamas ne rečiau kaip kartą per metus, taikant oficialias suderinimo procedūras, skirtas nustatyti ir išspręsti bet kokius neatitikimus. Įgyvendinamos laikmenų tvarkymo procedūros, siekiant apsaugoti jas nuo neteisėto atskleidimo, pakeitimo ar sunaikinimo per visą IRT turto gyvavimo ciklą, įskaitant saugaus saugojimo, perdavimo ir šalinimo būdus.

8.4. Informacijos saugumo incidentų valdymas

8.4.1. Bendrovė įgyvendina ir palaiko informacijos saugumo incidentų valdymo procesą, siekdama užtikrinti nuoseklų ir efektyvų požiūrį į informacijos saugumo incidentų valdymą.

8.4.2. Visi darbuotojai ir rangovai privalo nedelsdami pranešti apie visus pastebėtus ar įtariamus saugumo incidentus nustatytais pranešimo kanalais.

8.4.3. Saugumo incidentų metu įgyta patirtis dokumentuojama ir naudojama saugumo kontrolei ir incidentų reagavimo procedūroms tobulinti.

8.4.4.Bendrovė užtikrina struktūrizuotą bendravimą su atitinkamomis reguliavimo ir teisėsaugos institucijomis. Informacijos saugumo pareigūnas arba kiti paskirti atstovai atsako už atsakymus į oficialius užklausimus, reguliavimo audito rezultatus ir pranešimus apie saugumo incidentus pagal galiojančius įstatymus.

8.5. Kriptografija ir raktų valdymas

8.5.1. Bendrovė įgyvendina ir prižiūri kriptografines priemones, kad apsaugotų informacijos konfidencialumą, vientisumą ir autentiškumą per visą jos gyvavimo ciklą.

8.5.2. Visi jautrūs duomenys šifruojami tiek perdavimo, tiek saugojimo metu, naudojant pramonės standartų šifravimo algoritmus ir protokolus.

8.5.3. Bendrovė laikosi oficialios raktų valdymo politikos, apimančios visą kriptografinių raktų gyvavimo ciklą, įskaitant generavimą, platinimą, saugojimą, naudojimą, archyvavimą ir sunaikinimą.

8.5.4. Reguliariai atliekami kriptografinių diegimų vertinimai, siekiant užtikrinti atitiktį galiojantiems pramonės standartams ir geriausiai praktikai, kartu numatant dokumentais pagrįstas procedūras, kaip prireikus pereiti prie griežtesnių kriptografinių kontrolės priemonių.

8.6. Operacijų saugumas

8.6.1. Bendrovė, siekdama užtikrinti teisingas ir saugias operacijas, nustato ir palaiko dokumentuotas visų informacijos apdorojimo įrenginių veiklos procedūras.

8.6.2. Įdiegiamos pakeitimų valdymo procedūros, siekiant kontroliuoti visus informacijos apdorojimo įrenginių ir sistemų pakeitimus, taikant atitinkamus testavimo, dokumentavimo ir patvirtinimo reikalavimus.

8.6.3. Kūrimo, testavimo ir gamybos aplinkos atskiriamos, siekiant sumažinti neteisėtos prieigos prie operacinių sistemų ar jų modifikavimo riziką. Įdiegiamos sistemos ir saugumo kontrolės priemonės, siekiant aptikti neteisėtą informacijos apdorojimo veiklą, reguliariai peržiūrint ir analizuojant sistemos žurnalus.

8.6.4. Įdiegiama apsauga nuo kenkėjiškų programų reguliariai rengiant saugumo mokymus visiems vartotojams.

8.6.5. Prieš diegdama naujas technologijas, Bendrovė jas įvertina, patvirtina ir saugiai integruoja pagal rizikos valdymo, atitikties ir saugumo geriausios praktikos reikalavimus. Visos naujos technologijos įvertinamos dėl galimos saugumo rizikos, poveikio veiklai ir atitikties norminiams reikalavimams, įskaitant DORA ir ISO 27001.

8.7. Santykiai su tiekėjais

8.7.1. Bendrovė nustato ir palaiko informacijos saugumo reikalavimus santykiams su tiekėjais, kad sumažintų riziką, susijusią su tiekėjų prieiga prie organizacijos turto.

8.7.2. Oficialiose sutartyse ar susitarimuose numatomi konkretūs saugumo reikalavimai, įskaitant incidentų pranešimo įsipareigojimus, duomenų apsaugos reikalavimus ir audito teisių nuostatas, kaip nurodyta Trečiųjų šalių rizikos valdymo politikoje. Visos papildomos saugumo sąlygos atitinka Bendrovės politiką ir norminius reikalavimus.

8.7.3. Tiekėjų teikiamos paslaugos reguliariai stebimos ir peržiūrimos, o oficialūs tiekėjų taikomų saugumo priemonių vertinimai atliekami ne rečiau kaip kartą per metus.
8.7.4. Tiekėjų paslaugų pakeitimai valdomi taikant oficialias pakeitimų valdymo procedūras, o reikšmingų pakeitimų atveju atliekamas poveikio vertinimas.

8.8. Intelektinės nuosavybės teisė
8.8.1. Bet kokia intelektinė nuosavybė, įskaitant, bet neapsiribojant, programinę įrangą, šaltinio kodą, techninę dokumentaciją, dizainus, tyrimų duomenis, verslo strategijas ir patentus, kuriuos sukūrė, plėtojo ar patobulino darbuotojai, rangovai ar trečiosios šalys, naudodamos Bendrovės išteklius, laiką arba vykdydamos savo profesines pareigas, yra išimtinė Bendrovės nuosavybė, nebent rašytinėje sutartyje būtų nurodyta kitaip.
8.8.2. Darbuotojams, rangovams ir trečiųjų šalių paslaugų teikėjams griežtai draudžiama naudoti, kopijuoti, modifikuoti ar atskleisti bet kokią Bendrovės intelektinę nuosavybę asmeniniam naudojimui, platinimui išorėje ar neteisėtais komerciniais tikslais be aiškaus rašytinio Bendrovės vadovybės leidimo. Nutraukus darbo santykius ar sutartį, visa intelektinė nuosavybė, įskaitant šaltinio failus, dokumentus ir prieigos duomenis, turi būti grąžinta arba ištrinta pagal Bendrovės nurodymus.

9. INFORMACIJOS SAUGUMO POLITIKOS PERŽIŪRA

9.1. Ši Politika peržiūrima:
1) Ne rečiau kaip kas dvejus metus;
2) Įvykus reikšmingiems organizaciniams pokyčiams;
3) Po svarbių saugumo incidentų;
4) Nustačius naujas grėsmes ar pažeidžiamumus;
5) Pasikeitus norminiams reikalavimams;
6) Keičiantis technologijoms daroma įtaka saugumo reikalavimams.

9.2. Peržiūrint Politiką, atsižvelgiama į šiuos duomenis:
1) Informacinių sistemų audito rezultatus, įskaitant ankstesnių auditų rezultatus.
2) Nepriklausomų informacijos saugumo ekspertų rekomendacijas.
3) Reikšmingas grėsmes ir pažeidžiamumus informacinėse sistemose.
4) Informacijos saugumo incidentų ataskaitas.
5) Valdžios institucijų rekomendacijas.
6) Suinteresuotųjų šalių atsiliepimus.
7) Nepriklausomų peržiūrų rezultatus.
8) Prevencinių ir taisomųjų veiksmų būseną.
9) Ankstesnių vadovybės peržiūrų rezultatus.
10) Procesų vykdymą ir informacijos saugumo politikos laikymąsi.
11) Pakeitimus, turinčius įtakos Bendrovės požiūriui į informacijos saugumo valdymą, įskaitant organizacijos veiklos apimtį, verslo sąlygas, išteklių prieinamumą, sutartinius ar norminius reikalavimus ir techninę aplinką.
12) Grėsmių ir pažeidžiamumų tendencijas.
13) Užregistruotus informacijos saugumo incidentus.
14) Nepriklausomų šalių rekomendacijas.

9.3. Politikos peržiūrą atlieka informacijos saugumo pareigūnas, atsakingas už jos parengimą ir įgyvendinimą, įskaitant galimų Politikos nuostatų ir informacijos saugumo valdymo procesų patobulinimų vertinimą atsižvelgiant į pokyčius.
9.4. Informacijos saugumo politikos peržiūros rezultatai apima organizacinio požiūrio į informacijos saugumo valdymą tobulinimą, kontrolės priemonių ir jų tikslų koregavimą, išteklių paskirstymą ir atsakomybės paskirstymą.
9.5. Politikos peržiūra atliekama laikantis galiojančių teisės aktų.
9.6. Informacijos saugumo pareigūnas yra atsakingas už šios Politikos pakeitimus ir papildymus.
9.7. Patikslintą informacijos saugumo politiką tvirtina Bendrovės direktorius.

10. NORMINIAI AKTAI

10.1. Lietuvos Respublikos asmens duomenų teisinės apsaugos įstatymas
10.2. 2020 m. spalio 7 d. Europos Parlamento ir Tarybos reglamentas (ES) 2020/1503 dėl Europos sutelktinio finansavimo paslaugų verslui teikėjų, kuriuo iš dalies keičiamas Reglamentas (ES) 2017/1129 ir Direktyva (ES) 2019/1937 (Tekstas svarbus EEE)
10.3. Europos Parlamento ir Tarybos reglamentas (ES) 2022/2554 2022 m. gruodžio 14 d. dėl skaitmeninės veiklos atsparumo finansų sektoriuje, kuriuo iš dalies keičiami reglamentai (EB) Nr. 1060/2009, (ES) Nr. 648/2012, (ES) Nr. 600/2014, (ES) Nr. 909/2014 ir (ES) 2016/1011 (Tekstas svarbus EEE)

10.4. 2013 m. rugpjūčio 12 d. Europos Parlamento ir Tarybos direktyva 2013/40/ES dėl atakų prieš informacines sistemas (toliau – Kibernetinių nusikaltimų direktyva).
10.5. 2016 m. liepos 6 d. Europos Parlamento ir Tarybos direktyva (ES) 2016/1148 dėl priemonių aukštam bendram tinklų ir informacinių sistemų saugumo lygiui visoje Sąjungoje užtikrinti (toliau – TIS direktyva).
10.6. 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 (toliau – BDAR - Bendrasis duomenų apsaugos reglamentas).
10.7. Lietuvos Respublikos kibernetinio saugumo įstatymas
10.8. ISO/IEC 27001:2023 „Informacijos saugumas, kibernetinis saugumas ir privatumo apsauga. Informacijos saugumo valdymo sistemos. Reikalavimai“