					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P30S					Dokumento pavadinimas: **Reagavimo į incidentus politika**							
Versija: 1.0		Įsigaliojimo data: 01.01.2025			Dokumento savininkas:							
X	Politika		Standartas		Procedūra		Forma		Registras		Kita	

Peržiūrų istorija				
Peržiūros numeris	**Peržiūros data**	**Pakeitimai**	**Peržiūrėjo**	**Proceso savininkas**

Patvirtinimai			
Vardas	**Pareigos**	**Data**	**Parašas**

Suderinta su standartais ir reglamentais

Standartas / reglamentas	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	6.1, 6.3, 8 skyriai	Incidentų valdymas, nuolatinis tobulinimas, veiklos kontrolė
ISO/IEC 27002:2022	Kontrolės priemonės 5.24, 5.25	Incidentų aptikimas, pasirengimas, mokymasis
NIST SP 800-53 Rev.5	IR-4, IR-5, IR-6	Incidentų tvarkymas, stebėsena ir pranešimas
ES BDAR	33 straipsnis	Pranešimo apie pažeidimą reikalavimai
ES NIS2 direktyva	23 straipsnis	Privalomas pranešimas apie kibernetinius incidentus
ES DORA reglamentas	17 straipsnis	IRT incidentų valdymas
COBIT 2019	DSS02, DSS04	Paslaugų užklausų ir incidentų valdymas, veiklos tęstinumas

1. Tikslas

1.1. Ši politika nustato, kaip organizacija aptinka informacijos saugumo incidentus, apie juos praneša ir į juos reaguoja, kai jie daro poveikį jos skaitmeninėms sistemoms, duomenims ar paslaugoms.

1.2. Ji leidžia organizacijai sumažinti žalą, apsaugoti klientų duomenis ir vykdyti reglamentinius įpareigojimus, tokius kaip ES BDAR nustatytas 72 valandų terminas pranešti apie asmens duomenų saugumo pažeidimą.

1.3. Ši politika nustato aiškias atsakomybes, komunikacijos veiksmus ir poincidentinius veiksmus, įskaitant mažas organizacijas, neturinčias specializuotos saugumo komandos.

2. Taikymo sritis

2.1. Ši politika taikoma:

2.1.1. visiems darbuotojams, rangovams ir išorės IT paslaugų teikėjams;

2.1.2. visoms įmonės valdomoms sistemoms ir paslaugoms, įskaitant interneto svetaines, debesijos platformas, mobiliuosius įrenginius, nešiojamuosius kompiuterius ir el. pašto paskyras;

2.1.3. visų tipų incidentams, įskaitant:

2.1.3.1. neteisėtą prieigą prie duomenų ar sistemų;

2.1.3.2. kenkimo programinės įrangos infekcijas arba išpirkos reikalaujančią programinę įrangą;

2.1.3.3. fišingo ar socialinės inžinerijos bandymus;

2.1.3.4. sistemų nepasiekiamumą dėl kibernetinės atakos ar netinkamo naudojimo;

2.1.3.5. atsitiktinį jautrios informacijos atskleidimą arba ištrynimą;

2.1.3.6. veikloje naudojamų įrenginių ar duomenų laikmenų praradimą arba vagystę.

3. Tikslai

3.1. Nustatyti aiškų saugumo incidentų atpažinimo ir eskalavimo procesą.

3.2. Užtikrinti, kad apie incidentus būtų pranešama, jie būtų registruojami ir tvarkomi per iš anksto nustatytus terminus.

3.3. Užtikrinti greitą žalos lokalizavimą, duomenų atkūrimą ir paslaugų atkūrimą.

3.4. Užtikrinti, kad paveiktoms šalims, pavyzdžiui, klientams ar reguliuotojams, būtų pranešta, kai to reikalauja teisės aktai.

3.5. Užkirsti kelią pasikartojimui atliekant pagrindinės priežasties analizę, įgyvendinant korekcinius veiksmus ir tobulinant politiką.

3.6. Sudaryti sąlygas MVĮ atitikti ISO 27001 sertifikavimo reikalavimus ir audito metu įrodyti atskaitomybę.

4. Vaidmenys ir atsakomybės

4.1. Generalinis direktorius (GD)

4.1.1. Atsako už šią politiką ir užtikrina jos įgyvendinimą.

4.1.2. Prižiūri reagavimo į incidentus veiklą ir tvirtina pranešimus reguliuotojams ar klientams.

4.1.3. Peržiūri poincidentines ataskaitas ir užtikrina, kad prireikus politika būtų atnaujinta.

4.1.4. Gali deleguoti koordinavimo pareigas, tačiau išlaiko atskaitomybę.

4.2. IT paslaugų teikėjas / sistemų administratorius (vidinis arba išorės)

4.2.1. Aptinka ir tiria galimus saugumo incidentus.

4.2.2. Įgyvendina lokalizavimo ir atkūrimo veiksmus, pavyzdžiui, išjungia prieigą ir atkuria atsargines kopijas.

4.2.3. Apie visus patvirtintus arba įtariamus incidentus per 1 valandą nuo nustatymo informuoja GD.

4.2.4. Tvarko incidentų žurnalą, kuriame fiksuojamos laiko žymos, poveikio vertinimas ir reagavimo veiksmai.

[... 4.3–8 skyriai nėra įtraukti į šią peržiūrą. Įsigykite visą dokumentą, kad pasiektumėte visą turinį. ...]

9. Peržiūros ir atnaujinimo reikalavimai

9.1. Planinė peržiūra

9.1.1. Šią politiką bent kartą per 12 mėnesių turi peržiūrėti generalinis direktorius (GD), siekdamas užtikrinti:

9.1.1.1. suderinamumą su ISO/IEC 27001:2022 kontrolės priemonėmis;

9.1.1.2. reagavimą į naujas grėsmes, rizikas ir incidentus;

9.1.1.3. nuolatinę atitiktį teisiniams ir sutartiniams įpareigojimams, pavyzdžiui, ES BDAR ir DORA reglamentui.

9.2. Peržiūros inicijavimo įvykiai

9.2.1. Politika taip pat turi būti peržiūrėta ir atnaujinta po:

9.2.1.1. bet kurio didelio sunkumo incidento ar pranešimo reguliuotojui;

9.2.1.2. naujos IT infrastruktūros įdiegimo ar sistemų pakeitimų;

9.2.1.3. teisinių reikalavimų, susijusių su saugumo pažeidimais, pakeitimų.

9.3. Peržiūros dokumentavimas ir platinimas

9.3.1. Visos peržiūros ir pakeitimai turi būti dokumentuojami politikos pakeitimų žurnale.

9.3.2. Atnaujintos versijos turi būti išplatintos visiems darbuotojams, tiekėjams ir IT paslaugų teikėjams, dalyvaujantiems saugumo ar sistemų eksploatavimo veikloje.

9.3.3. Darbuotojų informuotumo įrodymai, pavyzdžiui, posėdžių protokolai ar patvirtinimai el. paštu, turi būti saugomi siekiant užtikrinti pasirengimą auditui.

10. Susijusios politikos ir sąsajos

10.1. Ši politika turi būti taikoma kartu su šiomis MVĮ politikomis:

10.1.1. P1S – Informacijos saugumo politika: nustato bendruosius lūkesčius dėl konfidencialumo, vientisumo ir prieinamumo užtikrinimo vykdant veiklą, įskaitant incidentų tvarkymą.

10.1.2. P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato įgaliojimų ir atskaitomybės struktūras, susijusias su incidentų aptikimu, pranešimu ir eskalavimu.

10.1.3. P4S – Prieigos kontrolės politika: sudaro sąlygas nedelsiant atšaukti prieigos teises vykdant reagavimo į incidentus veiksmus.

10.1.4. P8S – Informacijos saugumo supratimo ir mokymų politika: užtikrina, kad visi darbuotojai galėtų veiksmingai atpažinti saugumo incidentus ir apie juos pranešti.

10.1.5. P17S – Duomenų apsaugos ir privatumo politika: nustato teisinio pranešimo apie pažeidimą procedūras pagal ES BDAR ir padeda užtikrinti atitiktį reglamentiniams reikalavimams incidentų metu.

10.1.6. P22S – Žurnalų tvarkymo ir stebėsenos politika: suteikia reikiamas priemones ir matomumą saugumo įvykiams aptikti, analizuoti ir audituoti.

10.1.7. P31S – Įrodymų rinkimo ir kompiuterinės kriminalistikos politika: palaiko su incidentais susijusių veiksmų tyrimą ir teisinį pagrįstumą, nustatydama tinkamą įrodymų tvarkymą.

10.2. Šios politikos kartu sudaro MVĮ veiklos sistemą, skirtą informacijos saugumo incidentams aptikti, į juos reaguoti ir po jų atkurti veiklą.

11. Pamatiniai standartai ir sistemos

11.1. ISO/IEC 27001

11.1.1. 6.1 skyrius – reikalauja planuoti rizikos tvarkymą, įskaitant pasirengimą incidentams.

11.1.2. 6.3 skyrius – palaiko nuolatinį tobulinimą remiantis iš saugumo įvykių įgyta patirtimi.

11.1.3. 8.1 skyrius – pabrėžia veiklos kontrolę, skirtą incidentams ir sutrikimams valdyti.

11.2. ISO/IEC 27002

11.2.1. Kontrolės priemonė 5.24 – reikalauja struktūrizuoto požiūrio į pranešimą apie informacijos saugumo incidentus, jų vertinimą ir reagavimą į juos.

11.2.2. Kontrolės priemonė 5.25 – orientuota į mokymąsi iš incidentų, siekiant gerinti būsimą pasirengimą ir sistemų atsparumą.

11.3. NIST SP 800-53 Rev.5

11.3.1. IR-4 – apibrėžia incidentų tvarkymo procedūras, įskaitant lokalizavimą ir atkūrimą.

11.3.2. IR-5 – nustato incidentų stebėsenos ir analizės reikalavimus.

11.3.3. IR-6 – nustato privalomus išorinius ir vidinius incidentų pranešimo protokolus.

11.4. ES BDAR

11.4.1. 33 straipsnis – reikalauja per 72 valandas pranešti reguliuotojams apie asmens duomenų saugumo pažeidimus, nurodant apimtį ir rizikos mažinimo priemones.

11.5. ES NIS2 direktyva (2022/2555)

11.5.1. 23 straipsnis – reikalauja, kad esminiai ir svarbūs subjektai apie reikšmingus incidentus kompetentingoms institucijoms praneštų naudodami standartizuotus pranešimo formatus.

11.6. ES DORA reglamentas (2022/2554)

11.6.1. 17 straipsnis – reikalauja, kad finansų sektoriaus subjektai klasifikuotų, registruotų ir stebėtų su IRT susijusius incidentus ir sutrikimus.

11.7. COBIT 2019

11.7.1. DSS02 – Paslaugų užklausų ir incidentų valdymas: nustato gaires veiksmingam operacinių ir saugumo incidentų tvarkymui pagal valdysenos tikslus.

11.7.2. DSS04 – Veiklos tęstinumo valdymas: susieja reagavimą į incidentus su platesnėmis veiklos tęstinumo ir atkūrimo strategijomis.