					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P30					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	Komentaras
ISO/IEC 27001:2022	8 skyriaus 1 punktas, 9 skyrius	Struktūrizuoti rizikos valdymo ir reagavimo į incidentus procesai
ISO/IEC 27002:2022	Kontrolės priemonės 5.25–5.27	Incidentų vaidmenys, pranešimas, reagavimas ir tobulinimas
NIST SP 800-53 Rev.5	IR-1–IR-9	Išsamus reagavimo į incidentus gyvavimo ciklas
ES BDAR	33 straipsnio 1 dalis, 33 straipsnio 3 dalies a–d punktai, 34 straipsnio 1 dalis, 34 straipsnio 2 dalies a–c punktai	Pranešimo apie pažeidimus terminai, teikimas ir komunikacija su duomenų subjektais
ES NIS2 direktyva	23 straipsnio 1–4 dalys	Pranešimas nacionalinei institucijai ir struktūrizuotas ataskaitų teikimas
ES DORA reglamentas	17 straipsnio 1–3 dalys	Pranešimas apie didelius su IRT susijusius incidentus finansų sektoriaus subjektams
COBIT 2019	DSS02, DSS04, MEA	Apibrėžia incidentų valdymą, veiklos tęstinumą ir vertinimą, taip pat jų stebėseną ir vertinimą

1. Tikslas

1.1 Šia politika nustatoma formali informacijos saugumo incidentų, darančių poveikį organizacijai, identifikavimo, pranešimo apie incidentus, analizės, lokalizavimo, reagavimo, atkūrimo ir poincidentinio vertinimo sistema.

1.2 Ji užtikrina savalaikį, koordinuotą ir veiksmingą reagavimą, siekiant sumažinti veiklos sutrikimus, finansinius nuostolius, žalą reputacijai ir neatitiktį reglamentavimo reikalavimams.

1.3 Ši politika taip pat sudaro sąlygas nuolat gerinti organizacijos kibernetinį atsparumą, remiantis įgyta patirtimi ir integruojant po incidentų nustatytas išvadas į valdyseną, kontrolės priemones ir mokymo programas.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visam personalui, įskaitant darbuotojus, rangovus, konsultantus ir trečiųjų šalių paslaugų teikėjus

2.1.2 Visoms informacinėms sistemoms, taikomosioms programoms, infrastruktūrai, tinklams ir duomenims, nepriklausomai nuo to, ar jie yra vietiniai, debesijos ar hibridinėse aplinkose

2.1.3 Visų tipų saugumo incidentams, įskaitant, bet neapsiribojant:

2.1.3.1 Neteisėtą prieigą arba privilegijų eskalavimą

2.1.3.2 Kenkėjiškos programinės įrangos ir išpirkos reikalaujančios programinės įrangos atakas

2.1.3.3 Paslaugų trikdymo (DoS/DDoS) atakas

2.1.3.4 Duomenų praradimą, nutekėjimą arba neteisėtą iškėlimą

2.1.3.5 Netinkamą vidinį naudojimą arba politikų pažeidimus

2.1.3.6 Fizinio saugumo pažeidimus, darančius poveikį skaitmeniniam turtui

2.2 Politika apima aptikimą, triažą, tyrimą, eskalavimą, lokalizavimą, įrodymų tvarkymą, pranešimus, atkūrimą ir pagrindinės priežasties analizę.

3. Tikslai

3.1 Nustatyti pakartojamą ir plečiamą reagavimo į incidentus gebą, kuri leistų greitai aptikti, klasifikuoti ir suvaldyti saugumo incidentus.

3.2 Sumažinti saugumo įvykių poveikį veiklai, taikant struktūrizuotas lokalizavimo, pašalinimo ir sistemų atkūrimo procedūras.

3.3 Užtikrinti, kad pranešimas apie incidentus ir reagavimas atitiktų teisinius, reglamentavimo ir sutartinius reikalavimus, ypač susijusius su pranešimo apie pažeidimus terminais ir įrodymų tvarkymu.

3.4 Užtikrinti skaidrumą ir atskaitomybę, taikant tinkamą žurnalų tvarkymą, dokumentavimą ir rodiklių stebėseną visiems saugumo incidentams.

3.5 Skatinti nuolatinį tobulinimą, atliekant poincidentines peržiūras, įgyvendinant korekcinius veiksmus ir mokant suinteresuotąsias šalis.

4. Vaidmenys ir atsakomybės

4.1 Informacijos saugumo vadovas (CISO)

4.1.1 Valdo reagavimo į incidentus sistemą, užtikrina politikos įgyvendinimą ir prižiūri incidentų koordinavimą visos organizacijos mastu.

4.1.2 Didelių incidentų atveju veikia kaip pagrindinis kontaktinis asmuo ryšiams su reguliuotojais, vykdomąja vadovybe ir išorės teisininkais.

4.2 Reagavimo į incidentus koordinatorius

4.2.1 Koordinuoja tarpfunkcines reagavimo komandas, valdo darbo eigą ir stebi lokalizavimo bei atkūrimo būseną.

4.2.2 Inicijuoja ir vadovauja poincidentinei peržiūrai (PIR) bei užtikrina, kad korekciniai veiksmai būtų registruojami ir įgyvendinami.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Ši politika turi būti peržiūrima bent kartą per metus ir prireikus atnaujinama, kad būtų įtraukti:

9.1.1 Grėsmių aplinkos, incidentų tipų arba atakų vektorių pokyčiai

9.1.2 Iš didelių incidentų, beveik įvykusių atvejų arba reguliuotojų išvadų gauta įgyta patirtis

9.1.3 Taikomų teisės aktų ir reglamentų atnaujinimai (pvz., BDAR, DORA, NIS2)

9.1.4 Reagavimo į incidentus pratybų ir poincidentinių peržiūrų grįžtamasis ryšys

9.2 CISO atsako už peržiūros proceso inicijavimą ir koordinavimą, konsultuodamasis su:

9.2.1.1 Teisininku ir DAP

9.2.1.2 SOC ir IT operacijų komandomis

9.2.1.3 Veiklos tęstinumo ir rizikos valdymo komandomis

9.2.1.4 Vykdomąja vadovybe

9.3 Politikos pakeitimai turi būti:

9.3.1 Dokumentuojami saugykloje, valdomoje taikant versijų kontrolę

9.3.2 Komunikuojami visoms paveiktoms komandoms ir įtraukiami į informuotumo mokymus

9.3.3 Patvirtinami per stalo arba praktines reagavimo į incidentus pratybas per tris mėnesius nuo patvirtinimo

9.4 Skubūs atnaujinimai, inicijuoti dėl naujų grėsmių, audito išvadų arba naujai nustatytų teisinių įpareigojimų, turi būti įgyvendinami nedelsiant ir pažymimi politikos versijų istorijoje.

10. Susijusios politikos ir sąsajos

10.1 Šią politiką palaiko ir su ja susijusios šios organizacijos politikos:

10.1.1 P1 – Informacijos saugumo politika: nustato bendrą reikalavimą rizika grindžiamai ir incidentams pasirengusiai veiklai.

10.1.2 P5 – Pakeitimų valdymo politika: užtikrina, kad lokalizavimo ir atkūrimo veiklos, susijusios su infrastruktūra arba paslaugomis, būtų vykdomos pagal formalias procedūras.

10.1.3 P13 – Duomenų klasifikavimo ir ženklinimo politika: padeda klasifikuoti incidentų svarbą pagal duomenų jautrumą.

10.1.4 P15 – Atsarginių kopijų ir atkūrimo politika: sudaro sąlygas atkurti veiklą po išpirkos reikalaujančios programinės įrangos ar destruktyvių atakų, užtikrinant vientisumą.

10.1.5 P18 – Kriptografinių kontrolės priemonių politika: apibrėžia šifravimo priemones, kurios mažina incidentų poveikį ir duomenų atskleidimo riziką.

10.1.6 P22 – Žurnalų tvarkymo ir stebėsenos politika: užtikrina bazinį įvykių matomumą, perspėjimus ir žurnalų saugojimą, reikalingus veiksmingam aptikimui ir skaitmeninei kriminalistikai.

10.1.7 P29 – Testavimo duomenų ir testavimo aplinkų politika: užtikrina, kad incidentai, darantys poveikį neprodukcinėms sistemoms, taip pat būtų tvarkomi struktūrizuotai ir saugiai.

10.1.8 P33 – Audito ir atitikties stebėsenos politika: per struktūrizuotus auditus ir atitikties vertinimus patvirtina pasirengimą incidentams ir reagavimo veiksmingumą.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001: 8.1 punktas – operacinis planavimas ir kontrolė: struktūrizuoti procesai rizikoms valdyti ir reagavimui į incidentus planuoti.

11.2 ISO/IEC 27002:2022 – kontrolės priemonės 5.25–5.27: atsakomybės už incidentų valdymą, pranešimą apie incidentus, reagavimą, komunikaciją ir tobulinimą.

11.3 NIST SP 800-53 Rev.5: IR-1–IR-9, AU-6, PL-2: išsamūs reagavimo į incidentus gyvavimo ciklo, audito ir saugumo planavimo reikalavimai.

11.4 ES BDAR: 33 / 34 straipsniai: pareigos teikti pranešimus priežiūros institucijoms ir pranešti duomenų subjektams reikalavimai (su apibrėžtomis išimtimis).

11.5 ES NIS2 direktyva (2022/2555): 23 straipsnis: privalomas nacionalinis ataskaitų teikimas, įskaitant tarpinius ir galutinius pranešimus.

11.6 ES DORA reglamentas (2022/2554): 17 straipsnis: finansų įstaigų su IRT susijusių incidentų pranešimo institucijoms reikalavimai.

11.7 COBIT 2019: DSS02, DSS04, MEA01: paslaugų incidentų ir veiklos tęstinumo valdymas bei veiksmingumo ir atitikties stebėsena.