					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P39					Dokumento pavadinimas: **Koordinuoto pažeidžiamumų atskleidimo 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 teisės aktais

Standartas / reglamentas	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	6.1.3	
ISO/IEC 27002:2022	5.7, 8.8, 8.9, 8.28, 8.29	
NIST SP 800-53 Rev.5	RA-5, SI-2, PM-15, CA-8, SR-6	
ES BDAR	32 str. 1 d. d punktas	
NIS2 direktyva	21 str. 2 d. e punktas	
DORA reglamentas	11 str. 1 d. d punktas	
COBIT 2019	DSS05.01, DSS05.07, BAI09.02, MEA02.01	

1. Tikslas

1.1 Nustatyti formalų procesą informacijai apie pažeidžiamumus, darančius poveikį organizacijos sistemoms ar paslaugoms, gauti, tvarkyti ir atskleisti, kaip to reikalauja NIS2 direktyvos 21 straipsnio 2 dalies e punktas dėl pažeidžiamumų tvarkymo ir atskleidimo.

1.2 Skatinti išorės saugumo tyrėjus, partnerius ir naudotojus atsakingai pranešti apie pažeidžiamumus (koordinuotas pažeidžiamumų atskleidimas, CVD) ir apibrėžti, kaip organizacija teikia informaciją apie pažeidžiamumus suinteresuotosioms šalims.

2. Taikymo sritis

2.1 Ši politika taikoma visoms organizacijai priklausančioms arba jos valdomoms tinklo ir informacinėms sistemoms bei visiems šiose sistemose nustatytiems pažeidžiamumams.

2.2 Ji apima vidaus komandas (saugumo, IT ir kūrimo) ir visas išorės šalis, pranešančias apie pažeidžiamumus (pvz., tyrėjus, klientus, tiekėjus). Ji taip pat reglamentuoja komunikaciją su produktų tiekėjais ar paslaugų teikėjais, jei jų komponentai yra susiję su pažeidžiamumu.

3. Tikslai

3.1 Laiku nustatyti ir pašalinti saugumo pažeidžiamumus, pasitelkiant tiek vidaus vertinimus, tiek išorės atskleidimus.

3.2 Pateikti aiškias gaires išorės pranešėjams, kaip saugiai ir teisėtai pateikti informaciją apie pažeidžiamumus, o organizacijai – kaip veiksmingai reaguoti ir įgyvendinti taisomuosius veiksmus.

3.3 Užtikrinti atitiktį NIS2 direktyvos reikalavimams ir pramonės gerajai praktikai (ISO/IEC 29147 ir ISO/IEC 30111) koordinuoto pažeidžiamumų atskleidimo srityje, gerinant bendrą ekosistemos saugumą.

4. Vaidmenys ir atsakomybės

4.1 Pažeidžiamumų reagavimo komanda (VRT): paskirta komanda, vadovaujama vyriausiojo informacijos saugumo pareigūno arba pažeidžiamumų valdytojo, kuri priima ir atlieka pirminį pažeidžiamumų pranešimų vertinimą, įvertina riziką ir poveikį bei koordinuoja trūkumų šalinimą ir viešą atskleidimą.

4.2 IT ir kūrimo komandos: bendradarbiauja su VRT, kad patvirtintų praneštus pažeidžiamumus, parengtų ir išbandytų pataisas ar rizikos mažinimo priemones bei įdiegtų pataisymus. Prireikus pateikia techninę informaciją saugumo pranešimams.

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

9. Stebėsena ir auditas

9.1 VRT privalo tvarkyti pažeidžiamumų atskleidimo registrą, kuriame kiekvienas pranešimas sekamas nuo gavimo iki uždarymo. Šis registras peržiūrimas kas mėnesį, siekiant užtikrinti savalaikę atvirų klausimų pažangą. Pradelsti klausimai turi būti eskaluojami.

9.2 Vidaus auditas arba nepriklausomas saugumo vertintojas kasmet peržiūri pažeidžiamumų tvarkymo proceso veiksmingumą, pavyzdžiui, patikrina, ar pažeidžiamumų atvejų imtis buvo tvarkoma pagal politiką (gavimo patvirtinimas, ištaisymas, atskleidimas laiku). Taip pat turi būti patikrinta, ar viešai prieinamas atskleidimo kanalas veikia (pvz., ar testiniai el. laiškai yra gaunami ir į juos reaguojama).

9.3 Pažeidžiamumų rodikliai (apimtis pagal kritiškumą, taisymo terminai ir kt.) turi būti apibendrinami kas ketvirtį ir teikiami kibernetinio saugumo valdysenos komitetui, kad būtų galima atnaujinti rizikos vertinimą.

10. Peržiūra ir priežiūra

10.1 Ši politika peržiūrima ne rečiau kaip kartą per metus. Be to, bet koks reikšmingas IT aplinkos pokytis (pvz., naujos į internetą nukreiptos paslaugos paleidimas) arba reikšmingi reguliavimo pokyčiai (pvz., nauji ES teisės aktai dėl produktų pažeidžiamumų atskleidimo) turi inicijuoti neeilinę peržiūrą.

10.2 Atnaujinant politiką turi būti įtrauktas išorės pranešėjų grįžtamasis ryšys ir vidaus poincidentinių analizių įgyta patirtis. Esminius pakeitimus tvirtina vyriausiasis informacijos saugumo pareigūnas, jie komunikuojami visiems darbuotojams ir skelbiami organizacijos internetinėje saugumo politikų saugykloje, siekiant skaidrumo.

11. Susijusios politikos ir sąsajos

11.1 P01 – Informacijos saugumo politika. Nustato vadovybės įgaliojimus dėl pažeidžiamumų tvarkymo ir atskleidimo.

11.2 P19 – Pažeidžiamumų ir pataisų valdymo politika. Reguliuoja vidaus trūkumų šalinimo eigą, susietą su CVD pranešimų priėmimu.

11.3 P24 – Saugaus kūrimo politika. Užtikrina pataisų parengimą ir SDLC stiprinimą pagal gautus pranešimus.

11.4 P25 – Taikomųjų programų saugumo reikalavimų politika. Užtikrina, kad produktams būtų taikomi atskleidimui parengti saugumo reikalavimai.

11.5 P30 – Reagavimo į incidentus politika. Apima aktyvų atskleistų pažeidžiamumų išnaudojimą.

11.6 P31 – Įrodymų rinkimo ir kompiuterinės kriminalistikos politika. Užtikrina artefaktų iš praneštų ar išnaudotų trūkumų išsaugojimą.

11.7 P26 – Trečiųjų šalių ir tiekėjų saugumo politika. Koordinuoja atskleidimus, susijusius su tiekėjų komponentais.

11.8 P37 – Teisinės ir reguliacinės atitikties politika. Reguliuoja pranešimo, saugios veiklos išlygos formuluočių ir publikavimo reikalavimus.

12. Nuorodos

12.1 NIS2 direktyva (ES 2022/2555), 21 straipsnio 2 dalies e punktas (saugumas kūrimo metu ir pažeidžiamumų tvarkymas bei atskleidimas)

12.2 Komisijos įgyvendinimo reglamentas (ES) 2024/2690, priedo 6.10 skirsnis (techniniai reikalavimai pažeidžiamumų tvarkymo ir atskleidimo procesams)

12.3 ENISA techninės gairės dėl kibernetinio saugumo rizikos valdymo priemonių – skirsnis apie pažeidžiamumų tvarkymą ir atskleidimą

12.4 ISO/IEC 27001:2022 / ISO/IEC 27002:2022 (A.5.7 kontrolė dėl grėsmių žvalgybos ir pažeidžiamumų atskleidimo; A.8.28 kontrolė dėl saugaus kūrimo)

12.5 ISO/IEC 29147:2018 (pažeidžiamumų atskleidimo gairės) ir ISO/IEC 30111:2019 (pažeidžiamumų tvarkymo procesų gairės)