					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P19					Dokumento pavadinimas: **Pažeidžiamumų ir pataisų valdymo 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	8 skyrius	Sistemingas techninių pažeidžiamumų valdymas; nuolatinio saugumo kontrolės priemonių veiksmingumo užtikrinimas.
ISO/IEC 27002:2022	Kontrolės priemonės 8.8, 8.9, 5	Pataisų diegimo, pažeidžiamumų skenavimo, programinės įrangos vientisumo, saugios konfigūracijos ir turto apskaitos įgyvendinimo gairės.
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2, CM-6	Privalomi reguliarūs skenavimai, trūkumų šalinimas ir konfigūracijų valdymas.
ES BDAR	32 straipsnis, 49 konstatuojamoji dalis	Techninės priemonės, skirtos skubiam pataisų diegimui, pažeidžiamumų valdymui ir saugumo tęstinumui užtikrinti.
ES NIS2 direktyva	21 straipsnio 2 dalies d punktas	Pažeidžiamumų nustatymas, reagavimas ir mažinimas siekiant aukšto kibernetinės higienos lygio.
ES DORA reglamentas	8 straipsnis, 10 straipsnio 2 dalies f punktas	Savalaikis IRT pažeidžiamumų šalinimas; nuolatiniai grėsmėmis grindžiami vertinimai.
COBIT 2019	DSS05.02, DSS01.03, MEA	Techninių silpnybių skenavimas, stebėsena ir mažinimas; stebėsena dėl išnaudojimo požymių; veiksmingumo auditas, įskaitant pataisų būseną.

1. Tikslas

1.1 Ši politika nustato privalomuosius organizacijos reikalavimus techninių pažeidžiamumų ir programinės įrangos trūkumų nustatymui, klasifikavimui, šalinimui ir stebėsenai visose informacinėse sistemose ir turte, patenkančiuose į informacijos saugumo valdymo sistemos (ISVS) taikymo sritį.

1.2 Ji užtikrina, kad visi žinomi pažeidžiamumai būtų vertinami ir tvarkomi rizika grindžiamu ir savalaikiu būdu, taikant koordinuotą pataisų diegimą, konfigūracijos pakeitimus arba kompensacines kontrolės priemones, atsižvelgiant į verslo poreikius ir atitikties įpareigojimus.

1.3 Ši politika padeda užtikrinti atitiktį ISO/IEC 27001 A priedo 8 kontrolės priemonei ir ISO/IEC 27002 gairėms bei apima reglamentavimo reikalavimus pagal DORA 8 straipsnį, NIS2 21 straipsnį, BDAR 32 straipsnį ir COBIT 2019 DSS bei APO sritis.

2. Taikymo sritis

2.1 Ši politika taikoma visoms informacinėms sistemoms, turtui ir aplinkoms, kurios saugo, tvarko arba perduoda duomenis, kuriems taikoma ISVS valdysena, įskaitant:

2.1.1 operacines sistemas, taikomąsias programas, tinklo įrenginius, programinę aparatinę įrangą, debesijos platformas, taikomųjų programų sąsajas ir trečiųjų šalių programinę įrangą.

2.1.2 sistemas kūrimo, parengimo, gamybinėje, atsarginių kopijų ir atkūrimo po katastrofos aplinkose.

2.1.3 galinius įrenginius, serverius, IoT įrenginius, virtualizacijos infrastruktūrą ir konteinerius.

2.2 Ji yra privaloma:

2.2.1 vidaus darbuotojams: IT administratoriams, sistemų inžinieriams, taikomųjų programų kūrėjams, saugumo analitikams ir infrastruktūros komandoms.

2.2.2 išorės šalims: rangovams, valdomų paslaugų teikėjams (MSP), programinės įrangos tiekėjams ir sistemų integratoriams, turintiems technines atsakomybes už į taikymo sritį patenkantį turtą.

2.3 Politika apima visą pažeidžiamumų ir pataisų gyvavimo ciklą, įskaitant:

2.3.1 skenavimą ir nustatymą

2.3.2 rizikos klasifikavimą ir prioritetų nustatymą

2.3.3 pataisų gavimą, testavimą, diegimą ir grąžinimą į ankstesnę būseną

2.3.4 išimčių tvarkymą ir kompensacinių kontrolės priemonių planavimą

2.3.5 registravimą, ataskaitų teikimą ir audito atsekamumą

3. Tikslai

3.1 Užtikrinti, kad visi žinomi pažeidžiamumai būtų nustatyti, įvertinti ir pašalinti taip, kad būtų sumažinta rizikos ekspozicija ir išlaikytas suderinamumas su veiklos prioritetais.

3.2 Nustatyti nuoseklius, visos organizacijos mastu taikomus pažeidžiamumų skenavimo, kritiškumo klasifikavimo (pvz., CVSS) ir pataisų valdymo procesus, įskaitant skubių atvejų tvarkymą ir grąžinimo į ankstesnę būseną planavimą.

3.3 Sudaryti sąlygas saugiam konfigūracijų valdymui, užtikrinant suderinamumą su saugumo stiprinimo baziniais reikalavimais, pakeitimų kontrolės praktikomis ir realiojo laiko grėsmių žvalgyba.

3.4 Užtikrinti išmatuojamą atitiktį reglamentavimo ir standartų kontrolės priemonėms, susijusioms su sistemų vientisumu, tinkamu pataisų valdymu ir savalaikiu trūkumų šalinimu.

3.5 Apibrėžti atsakomybę ir atskaitomybę pagal vaidmenis visame pažeidžiamumų valdymo gyvavimo cikle, užtikrinant, kad visos suinteresuotosios šalys veiktų pagal nustatytus SLA ir teiktų ataskaitas pagal nustatytus kontrolės rodiklius.

3.6 Stiprinti pasirengimą auditui ir didinti atsparumą kylančioms grėsmėms, įskaitant nulinės dienos pažeidžiamumus, aktyvias išnaudojimo grandines ir didelio poveikio tiekėjų atskleidimus.

4. Vaidmenys ir atsakomybės

4.1 Vyriausiasis informacijos saugumo pareigūnas

4.1.1 Atsako už šią politiką ir užtikrina jos integravimą į ISVS.

4.1.2 Nustato organizacijos rizikos laikyseną ir užtikrina suderinamumą su reglamentavimo ir kontrolės lūkesčiais.

4.2 Pažeidžiamumų valdymo vadovas / saugumo operacijų vadovas

4.2.1 Prižiūri visą pažeidžiamumų ir pataisų valdymo veiklą nuo pradžios iki pabaigos.

4.2.2 Koordinuoja skenavimo grafikus, prioritetų nustatymo modelius ir trūkumų šalinimo terminus.

4.2.3 Prižiūri pažeidžiamumų registrą ir bendradarbiauja vertinant kompensacines kontrolės priemones.

[... 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 arba įvykus bent vienai iš šių aplinkybių:

9.1.1 reikšmingi reglamentavimo atnaujinimai (pvz., DORA, NIS2 pakeitimai)

9.1.2 pažeidžiamumų prioritetų nustatymo sistemų pakeitimai (pvz., CVSS atnaujinimai)

9.1.3 reikšmingi IT aplinkos pakeitimai (pvz., migravimas į debesiją, esminis EDR pertvarkymas)

9.1.4 didelio atgarsio sulaukę pažeidimai arba išoriniai pranešimai, dėl kurių būtina stiprinti politiką

9.2 Peržiūras turi atlikti CISO, bendradarbiaudamas su saugumo operacijų, rizikos valdymo ir infrastruktūros vadovybe.

9.3 Politikos atnaujinimai turi būti:

9.3.1 dokumentuojami ISVS dokumentų kontrolės registre

9.3.2 peržiūrėti ir patvirtinti vadovybės

9.3.3 komunikuojami visoms paveiktoms suinteresuotosioms šalims, įskaitant trečiųjų šalių duomenų tvarkytojus

9.4 Istorinės versijos turi būti saugiai saugomos audito ir atskaitomybės tikslais.

10. Susijusios politikos ir sąsajos

10.1 P1 - Informacijos saugumo politika. Nustato bendrą įsipareigojimą apsaugoti sistemas ir duomenis, įskaitant proaktyvų pažeidžiamumų valdymą ir programinės įrangos vientisumo užtikrinimą.

10.2 P5 - Pakeitimų valdymo politika. Reglamentuoja visą pataisų diegimą ir konfigūracijos pakeitimus, reikalaudama dokumentavimo, testavimo, patvirtinimo ir grąžinimo į ankstesnę būseną procedūrų, papildančių pažeidžiamumų šalinimo procesus.

10.3 P6 - Rizikos valdymo politika. Palaiko nepašalintų pažeidžiamumų klasifikavimą ir tvarkymą, taikant struktūrizuotus rizikos vertinimus, poveikio analizę ir likutinės rizikos priėmimo procedūras.

10.4 P12 - Turto valdymo politika. Užtikrina, kad sistemos būtų tiksliai apskaitomos ir klasifikuojamos, sudarant sąlygas nuosekliam pažeidžiamumų skenavimui, savininkų priskyrimui ir pataisų aprėpčiai per visą gyvavimo ciklą.

10.5 P22 - Žurnalų tvarkymo ir stebėsenos politika. Nustato reikalavimus įvykių nustatymui ir audito pėdsako generavimui. Ši politika užtikrina matomumą į pataisų diegimo veiklą, nesankcionuotus pakeitimus ir bandymus išnaudoti žinomus pažeidžiamumus.

10.6 P30 - Reagavimo į incidentus politika. Nustato eskalavimo protokolus ir lokalizavimo strategijas išnaudotų pažeidžiamumų, pažeidimų tyrimų ir korekcinių veiksmų atvejais, suderintus su šios politikos kontrolės priemonėmis.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001: 8.1 skyrius - Veiklos planavimas ir kontrolė: reikalauja sistemingai tvarkyti techninius pažeidžiamumus siekiant užtikrinti nuolatinį saugumo kontrolės priemonių veiksmingumą.

11.2 ISO/IEC 27002:2022 - Kontrolės priemonės 8.8, 8.9, 5: pateikia pataisų diegimo, pažeidžiamumų skenavimo, programinės įrangos vientisumo ir integracijos su saugia konfigūracija bei turto apskaita įgyvendinimo gaires.

11.3 NIST SP 800-53 Rev.5: RA-5 - Pažeidžiamumų stebėsena ir skenavimas: nustato reguliarų skenavimą ir trūkumų šalinimo stebėseną. SI-2 - Trūkumų šalinimas: reikalauja skubiai įvertinti ir mažinti trūkumus taikant turimas pataisas ar kitus veiksmus. CM-2 / CM-6 - Konfigūracijų valdymo bazės ir kontrolės priemonės: nustato pagrindą saugioms sistemų konfigūracijoms, susietoms su privalomu pataisų taikymu.

11.4 ES BDAR (2016/679): 32 straipsnis - Tvarkymo saugumas: reikalauja įgyvendinti tinkamas technines priemones, tokias kaip skubus pataisų diegimas ir pažeidžiamumų valdymas, siekiant užtikrinti konfidencialumą ir sistemų atsparumą. 49 konstatuojamoji dalis: skatina subjektus įgyvendinti prevencines kontrolės priemones prieš žinomas grėsmes, kad būtų palaikomas saugumas ir tęstinumas.

11.5 ES NIS2 direktyva (2022/2555): 21 straipsnio 2 dalies d punktas: įpareigoja esminius ir svarbius subjektus nustatyti sistemų pažeidžiamumus, į juos reaguoti, juos mažinti ir palaikyti aukštą kibernetinės higienos lygį.

11.6 ES DORA reglamentas (2022/2554): 8 straipsnis - IRT rizikos valdymas: reikalauja nustatyti ir laiku šalinti pažeidžiamumus informacijos ir ryšių technologijose, naudojamose finansinėse sistemose. 10 straipsnio 2 dalies f punktas: pabrėžia nuolatinius grėsmėmis grindžiamus pažeidžiamumų vertinimus ir pataisų diegimą kaip operacinio atsparumo dalį.

11.7 COBIT 2019: DSS05.02 - Saugumo pažeidžiamumų valdymas: nurodo organizacijoms skenuoti, stebėti ir mažinti žinomas technines silpnybes. DSS01.03 - Infrastruktūros stebėsena: užtikrina, kad sistemos būtų stebimos dėl išnaudojimo ar silpnybių požymių. MEA03 - Atitikties stebėsena, vertinimas ir analizė: reikalauja reguliariai audituoti kontrolės priemonių veiksmingumą, įskaitant pataisų būseną ir išimčių tvarkymą.