					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P19S					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	Komentaras
ISO/IEC 27001:2022	8 skyrius	
ISO/IEC 27002:2022	Kontrolės priemonės 8.8, 8.9	
NIST SP 800-53 Rev.5	RA-5, SI-2, CM-2	
ES NIS2 direktyva	21 straipsnio 2 dalies d ir e punktai	
ES DORA reglamentas	8 straipsnio 1 dalis, 10 straipsnio 2 dalis	
COBIT 2019	DSS05.02, APO12	
ES BDAR	32 straipsnio 1 dalies b punktas	

1. Tikslas

1.1 Ši politika nustato, kaip organizacija identifikuoja, vertina ir mažina pažeidžiamumus sistemose, taikomosiose programose ir infrastruktūroje.

1.2 Jos tikslas – mažinti kibernetinio saugumo riziką, užtikrinant savalaikį pataisų diegimą ir rizika grindžiamą taisomųjų veiksmų taikymą, tinkamą mažosioms ir vidutinėms įmonėms (MVĮ).

1.3 Ši politika padeda užtikrinti atitiktį ISO/IEC 27001:2022 sertifikavimo reikalavimams ir vykdyti reglamentavimo įpareigojimus pagal ES BDAR, NIS2 direktyvą ir DORA reglamentą, nustatydama proaktyvų techninių pažeidžiamumų valdymą.

1.4 Organizacija pripažįsta, kad neįdiegtos pataisos sistemose kelia reikšmingą grėsmę informacijos saugumui ir turi būti valdomos sistemiškai bei nedelsiant.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visiems organizacijos naudojamiems serveriams, staliniams kompiuteriams, nešiojamiesiems kompiuteriams, mobiliesiems įrenginiams, tinklo įrangai ir debesijos platformoms;

2.1.2 visoms operacinėms sistemoms, trečiųjų šalių programinei įrangai, papildiniams ir taikomosioms programoms, naudojamoms vykdant veiklą;

2.1.3 vidaus IT darbuotojams ir išorės paslaugų teikėjams, atsakingiems už sistemų priežiūrą, atnaujinimus ar stebėseną;

2.1.4 bet kokiam organizacijos arba jos vardu prižiūrimam individualiai sukurtam programiniam kodui ar įterptajai programinei įrangai.

2.2 Politika apima tiek organizacijos tiesiogiai valdomą infrastruktūrą, tiek sistemas, kurias administruoja sutartiniai tiekėjai ar prieglobos paslaugų teikėjai.

3. Tikslai

3.1 laiku ir nuosekliai identifikuoti bei vertinti žinomus pažeidžiamumus visuose IT ištekliuose;

3.2 taikyti pataisas ir programinės įrangos atnaujinimus pagal jų kritiškumą ir riziką organizacijos veiklai ar asmens duomenims;

3.3 užkirsti kelią techninių silpnybių išnaudojimui, kuris gali lemti paslaugų sutrikimą, duomenų saugumo pažeidimą ar neatitiktį teisiniams reikalavimams;

3.4 tvarkyti tikslius įrašus apie įdiegtas pataisas, neišspręstas problemas ir išimtis, kad būtų užtikrintas pasirengimas auditui;

3.5 naudoti organizacijos dydį ir veiklos sudėtingumą atitinkančias priemones ir procesus, nemažinant veiksmingumo;

3.6 užtikrinti teisinę ir reglamentavimo atitiktį, įskaitant ES BDAR 32 straipsnį ir ISO/IEC 27001 A priedo 8 srities kontrolės priemones.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GV)

4.1.1 atsako už bendrą priežiūrą, kad pataisų diegimo ir pažeidžiamumų valdymo veiklos būtų įgyvendinamos;

4.1.2 tvirtina rizikos išimtis, kai pataisų pritaikyti negalima, ir peržiūri susijusias riziką mažinančias apsaugos priemones;

4.1.3 peržiūri pataisų būsenos ataskaitas ir užtikrina, kad būtų skirti ištekliai pataisų diegimo reikalavimams vykdyti.

4.2 IT paslaugų teikėjas / vidaus IT administratorius

4.2.1 stebi sistemas dėl pažeidžiamumų ir prieinamų pataisų, naudodamas tiekėjų pranešimus, saugumo biuletenius ir operacinių sistemų lygmens įspėjimus;

4.2.2 diegia operacinių sistemų, programinės aparatinės įrangos ir taikomųjų programų atnaujinimus per nustatytus terminus;

4.2.3 tvarko formalų pataisų žurnalą ir dokumentuoja neišspręstus arba atidėtus atnaujinimus;

4.2.4 atlieka kritinių atnaujinimų testavimą ir planavimą, kad būtų sumažinti veiklos sutrikimai.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Kasmetinė peržiūra

9.1.1 Ši politika turi būti peržiūrima bent kartą per metus Generalinio vadovo, atsižvelgiant į IT paslaugų teikėjo ir privatumo koordinatoriaus pateiktą informaciją.

9.2 Peržiūros prielaidos

9.2.1 Tarpinės peržiūros turi būti atliekamos, jei:

9.2.1.1 didelio poveikio pažeidžiamumas arba jo išnaudojimas paveikia į taikymo sritį patenkančias sistemas;

9.2.1.2 įvyksta reikšmingi sistemų ar programinės įrangos pokyčiai;

9.2.1.3 auditas nustato pataisų diegimo procesų spragas;

9.2.1.4 užregistruojamas su pataisų diegimu susijęs incidentas arba pažeidimas.

9.3 Politikos versijų kontrolė

9.3.1 Visi atnaujinimai turi būti registruojami versijų žurnale, pateikiant pakeitimų santrauką.

9.3.2 Pakeitimai turi būti komunikuojami susijusiam personalui.

9.3.3 Pasenusios versijos turi būti archyvuojamos taikant ribotą prieigą.

10. Susijusios politikos ir sąsajos

10.1 Ši politika remia ir yra susijusi su keliomis kitomis MVĮ politikomis:

10.1.1 P12S – Turto valdymo politika: nustato sistemų savininkystę ir klasifikaciją, užtikrindama, kad visas turtas, kuriam reikia taikyti pataisas, būtų apskaitytas ir įtrauktas į turto registrą;

10.1.2 P14S – Duomenų saugojimo ir sunaikinimo politika: užtikrina, kad sistemoms, kurių eksploatavimas nutraukiamas, būtų saugiai pritaikyti atnaujinimai arba atliktas saugus išvalymas, taip sumažinant pažeidžiamumų poveikį;

10.1.3 P17S – Duomenų apsaugos ir privatumo politika: nustato pažeidžiamumų šalinimo prioritetus sistemoms, kuriose tvarkomi asmens duomenys, siekiant laikytis privatumo teisės aktų;

10.1.4 P22S – Žurnalų tvarkymo ir stebėsenos politika: padeda aptikti neįdiegtas pataisas turinčias sistemas arba įtartiną elgseną, kuri gali rodyti pažeidžiamumo išnaudojimą;

10.1.5 P30S – Reagavimo į incidentus politika: nustato reagavimo į pažeidžiamumus, dėl kurių kyla saugumo incidentai, procedūras, įskaitant eskalavimo ir pranešimo veiksmus.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8 skyrius – reikalauja valdyti operacinę riziką, įskaitant pažeidžiamumų valdymą, taikant atitinkamas kontrolės priemones.

11.2 ISO/IEC 27002

11.2.1 Kontrolės priemonė 8.8 – nustato procesus, skirtus sistemose žinomoms techninėms silpnybėms nustatyti ir šalinti.

11.2.2 Kontrolės priemonė 8.9 – pabrėžia saugią konfigūraciją, pataisų tikrinimą ir pakeitimų valdymą, kad atnaujinimų metu būtų išvengta naujo pažeidžiamumo.

11.3 NIST SP 800-53 Rev.5

11.3.1 RA-5 – reikalauja identifikuoti pažeidžiamumus ir pašalinti juos per nustatytus terminus.

11.3.2 SI-2 – įpareigoja operatyviai taikyti pataisas ir atnaujinimus pagal jų kritiškumą.

11.3.3 CM-2 – reglamentuoja bazinių konfigūracijų valdymą ir atnaujinimų dokumentavimą, siekiant užtikrinti nuoseklias apsaugos priemones.

11.4 ES BDAR

11.4.1 32 straipsnio 1 dalies b punktas – reikalauja, kad organizacijos įgyvendintų tinkamas technines priemones, įskaitant pataisų diegimą, siekdamos užtikrinti tvarkymo saugumą.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies d punktas – reikalauja valdyti pažeidžiamumus taikant sistemingą nustatymą ir šalinimą.

11.5.2 21 straipsnio 2 dalies e punktas – įpareigoja užtikrinti saugią konfigūraciją ir pataisų valdymą, siekiant IRT atsparumo.

11.6 ES DORA reglamentas

11.6.1 8 straipsnio 1 dalis – reikalauja nustatyti ir mažinti IRT riziką, įskaitant techninius pažeidžiamumus.

11.6.2 10 straipsnio 2 dalis – įpareigoja finansų sektoriaus subjektus šalinti silpnybes, darančias poveikį IRT sistemoms ir veiklai.

11.7 COBIT 2019

11.7.1 DSS05.02 – reikalauja valdyti žinomus techninius pažeidžiamumus, siekiant palaikyti saugias operacijas.

11.7.2 APO12 – susieja rizikos valdymą su proaktyvia sistemų silpnybių stebėsena ir šalinimu.