					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P33S					Dokumento pavadinimas: **Audito ir atitikties stebėsenos 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	Punktas / straipsnis	Komentaras
ISO/IEC 27001:2022	9.2, 10 punktai	Vidaus auditai, nuolatinis tobulinimas ir neatitikčių šalinimas
ISO/IEC 27002:2022	5.35, 5.37 kontrolės priemonės	Planinės vidaus peržiūros, nepriklausomos išorės procesų peržiūros
NIST SP 800-53 Rev.5	CA-2, CA-7, AU-6	Saugumo vertinimai, nuolatinė stebėsena, audito peržiūra, analizė ir ataskaitų teikimas
ES BDAR	24 ir 32 straipsniai	Techninių ir organizacinių priemonių auditas, kontrolės priemonių veiksmingumo įrodymai
ES NIS2 direktyva	21 straipsnio 2 dalies f punktas	Aktyvi peržiūra ir įrodymais grindžiama atitiktis
ES DORA reglamentas	10 straipsnis	IRT rizikos valdymas, stebėsena ir ataskaitų teikimas
COBIT 2019	MEA01, MEA03	Stebėsena, atitikties vertinimas, pasirengimas trečiųjų šalių peržiūroms

1. Tikslas

1.1 Ši politika nustato organizacijos požiūrį į vidaus auditų vykdymą, saugumo kontrolės priemonių patikras ir atitikties teisės aktų bei kitų reikalavimų stebėseną. Ji užtikrina, kad visos kontrolės priemonės, politikos, sistemos ir paslaugų teikėjai būtų reguliariai ir struktūruotai peržiūrimi.

1.2 Tikslas – nustatyti kontrolės priemonių neveiksmingumą, užkirsti kelią neatitikčiai ir įrodyti deramą rūpestingumą pagal ISO/IEC 27001, ES BDAR ir susijusias sistemas.

1.3 Ši politika sudaro sąlygas MVĮ išlaikyti veiklos kontrolę ir pasirengimą sertifikavimui net ir neturint atskiro atitikties padalinio, taikant paprastus, pakartotinai naudojamus kontrolinius sąrašus ir pagal riziką prioritetizuojant išvadas.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visiems vidaus padaliniams ir išorės paslaugų teikėjams, kurių atsakomybė susijusi su IT sistemomis, asmens duomenimis ir verslui kritinėmis paslaugomis;

2.1.2 visoms kontrolės priemonėms ir sistemoms, patenkančioms į informacijos saugumo valdymo sistemos taikymo sritį;

2.1.3 visiems vidaus auditams, saugumo kontrolės priemonių peržiūroms ir atitikties patikroms, neatsižvelgiant į tai, ar jas atlieka organizacija, išorės konsultantas, klientas ar reguliavimo institucija.

2.2 Ši politika taip pat taikoma įrodymų rinkimui ir ataskaitų teikimui, susijusiam su:

2.2.1 ISO/IEC 27001 sertifikavimo ir pakartotinio sertifikavimo auditais;

2.2.2 duomenų apsaugos auditais pagal ES BDAR arba sutartinius įsipareigojimus;

2.2.3 kliento inicijuotais saugumo klausimynais arba deramo patikrinimo peržiūromis;

2.2.4 bet kokiomis reguliavimo institucijų arba nepriklausomomis peržiūromis pagal NIS2 direktyvą ar DORA reglamentą, kai taikoma.

3. Tikslai

3.1 Užtikrinti, kad visos pagrindinės kontrolės priemonės ir politikos būtų reguliariai peržiūrimos dėl veiksmingumo ir atitikties.

3.2 Užtikrinti audito pėdsaką ir korekcinių veiksmų įrašus, leidžiančius pagrįsti atskaitomybę ir tobulinimą.

3.3 Pasirengti sertifikavimui, pakartotiniam sertifikavimui ir klientų patikinimo programoms, pvz., ISO 27001 ar tiekėjų vertinimui.

3.4 Anksti nustatyti spragas, kad taisomieji veiksmai būtų įgyvendinami nedelsiant, dar prieš problemoms išaugant ar sukeliant įsipareigojimų pažeidimą.

3.5 Sudaryti sąlygas generaliniam vadovui ir IT paslaugų teikėjui koordinuoti peržiūras su minimalia administracine našta, kartu užtikrinant pagrįstus rezultatus.

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GM)

4.1.1 prižiūri audito programą;

4.1.2 tvirtina vidaus peržiūrų planus ir audito išvadas;

4.1.3 priskiria korekcinius veiksmus ir stebi jų įgyvendinimą;

4.1.4 tvirtina išorės auditorių ar konsultantų pasitelkimą.

4.2 Išorės IT paslaugų teikėjas / administratorius

4.2.1 teikia įrodymus vidaus ir išorės auditų metu, pvz., žurnalus, konfigūracijas ir prieigos kontrolės įrašus;

4.2.2 padeda atlikti technines patikras, pvz., atsarginių kopijų būsenos ir pataisų diegimo atitikties patikrinimą;

4.2.3 prižiūri audito įrodymų saugyklą.

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Metinė politikos ir audito plano peržiūra

9.1.1 Generalinis vadovas (GM) privalo peržiūrėti šią politiką ir audito grafiką ne rečiau kaip kartą per metus.

9.1.2 Peržiūros metu turi būti įvertinta:

9.1.2.1 auditų veiksmingumas nustatant spragas;

9.1.2.2 auditų ir korekcinių veiksmų užbaigimo rodiklis;

9.1.2.3 taikomų teisinių, reguliacinių ar sertifikavimo reikalavimų pokyčiai.

9.2 Atnaujinimai pagal inicijavimo įvykius

9.2.1 Politika turi būti peržiūrima ir atnaujinama, kai:

9.2.2 sertifikavimo arba priežiūros audito metu nustatomas esminis neatitikimas;

9.2.3 pasikeičia teisinės ar reguliacinės sistemos, pvz., naujos ES BDAR gairės ar nacionalinis NIS2 direktyvos įgyvendinimas;

9.2.4 verslo pokyčiai daro poveikį sistemoms, procesams ar tiekėjams, įtrauktiems į audito taikymo sritį;

9.2.5 kritinis incidentas ar pažeidimas atskleidžia anksčiau nenustatytas kontrolės priemonių spragas.

9.3 Atnaujinimų dokumentavimas

9.3.1 Visi pakeitimai turi būti registruojami politikos versijų kontrolės žurnale.

9.3.2 Atnaujinimai turi būti išplatinti visiems komandos nariams, dalyvaujantiems audituose.

9.3.3 Siekiant užtikrinti supratimą, kartu su atnaujinta politika turi būti pateikta pakeitimų santrauka.

10. Susijusios politikos ir sąsajos

10.1 Šią politiką palaiko ir sustiprina kelios kitos MVĮ politikos:

10.1.1 P1S – Informacijos saugumo politika: nustato bazinius visų kontrolės priemonių reikalavimus ir numato jų laikymosi užtikrinimą auditais.

10.1.2 P2S – Valdysenos vaidmenų ir atsakomybių politika: nustato atskaitomybę už audito planavimą, vykdymą ir korekcinių veiksmų valdymą.

10.1.3 P6S – Rizikos valdymo politika: apima auditų metu nustatytus kontrolės priemonių trūkumus ir užtikrina, kad audito išvados būtų dokumentuojamos rizikų registre.

10.1.4 P17S – Duomenų apsaugos ir privatumo politika: apibrėžia pagal ES BDAR audituotinas kontrolės priemones, įskaitant duomenų tvarkymą, reagavimą į pažeidimus ir privatumo pranešimus.

10.1.5 P22S – Žurnalų valdymo ir stebėsenos politika: nustato audito žurnalų ir kriminalistinių duomenų, naudojamų atliekant atitikties ir kontrolės priemonių peržiūras, tvarką.

10.1.6 P30S – Reagavimo į incidentus politika: reikalauja periodiškai audituoti incidentų įrašus ir poincidentines peržiūras, siekiant patikrinti reagavimo veiksmingumą.

10.1.7 P31S – Įrodymų rinkimo ir kriminalistikos politika: nustato procedūras, skirtas auditų metu rinkti patikrinamus įrodymus, užtikrinant perdavimo grandinės dokumentavimą.

10.2 Kartu šios politikos sukuria uždarą kontrolės aplinką, kuri sudaro sąlygas vidaus patikrai, išoriniam patikinimui ir su standartais suderintai valdysenai.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001:

11.1.1 9.2 punktas – reikalauja atlikti vidaus auditus, kuriais vertinamas ISVS veiksmingumas ir atitiktis reikalavimams.

11.1.2 10.1 punktas – nustato nuolatinio tobulinimo pareigą, grindžiamą audito rezultatais ir neatitikčių šalinimu.

11.2 ISO/IEC 27002:

11.2.1 5.35 kontrolės priemonė – reikalauja planinių vidaus kontrolės priemonių ir procesų peržiūrų.

11.2.2 5.37 kontrolės priemonė – pabrėžia nepriklausomų peržiūrų svarbą, ypač išorės procesams.

11.3 NIST SP 800-53 Rev.5:

11.3.1 CA-2 – Saugumo vertinimai: reikalauja audituoti įgyvendintas kontrolės priemones, siekiant patvirtinti jų veiksmingumą.

11.3.2 CA-7 – Nuolatinė stebėsena: pabrėžia aktyvų kontrolės priemonių trūkumų nustatymą ir peržiūrą.

11.3.3 AU-6 – Audito peržiūra, analizė ir ataskaitų teikimas: reikalauja reguliariai analizuoti audito žurnalus ir audito išvadas bei užtikrinti jų ištaisymą.

11.4 ES BDAR:

11.4.1 24 ir 32 straipsniai – reikalauja įgyvendinti ir audituoti technines ir organizacines priemones, įskaitant kontrolės priemonių veiksmingumo įrodymus ir jų tobulinimą laikui bėgant.

11.5 ES NIS2 direktyva (2022/2555):

11.5.1 20–21 straipsniai – reikalauja aktyvios kontrolės priemonių peržiūros, įrodymais grindžiamos atitikties ir audituojamumo esminiams ir svarbiems subjektams.

11.6 COBIT 2019:

11.6.1 MEA01 – Veiksmingumo ir atitikties stebėsena, vertinimas ir analizė: reikalauja periodiškai vertinti procesų ir kontrolės priemonių veiksmingumą pagal standartus ir tikslus.

11.6.2 MEA03 – Atitikties išorės reikalavimams užtikrinimas: daugiausia dėmesio skiria vidaus stebėsenai ir pasirengimui trečiųjų šalių auditams bei reguliavimo institucijų peržiūroms.