					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P33					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	Skyrius / straipsnis	Pastaba
ISO/IEC 27001:2022	9.2, 9.3, 10 skyriai	
ISO/IEC 27002:2022	Kontrolės priemonės 5.35–5.37	
NIST SP 800-53 Rev.5	CA-2, CA-5, CA-7	
ES BDAR	24, 32, 33 straipsniai	
ES NIS2 direktyva	21 straipsnio 2 dalies g punktas, 27 straipsnis	
ES DORA reglamentas	10 straipsnio 2 dalies e punktas, 25 straipsnis	
COBIT 2019	MEA01, MEA03	

1. Tikslas

1.1 Šios politikos tikslas – nustatyti ir reglamentuoti organizacijos audito ir atitikties stebėsenos programą, siekiant:

1.1.1 patvirtinti saugumo ir privatumo kontrolės priemonių veiksmingumą

1.1.2 užtikrinti atitiktį taikomiems standartams, teisiniams reikalavimams ir sutartiniams įsipareigojimams

1.1.3 laiku nustatyti neatitiktis, neveiksmingumą ir atitikties rizikas

1.1.4 remti nuolatinį tobulinimą ir pasirengimą sertifikavimui, vertinimams ir reguliavimo institucijų peržiūroms

1.2 Ši politika palaiko informacijos saugumo valdymo sistemos (ISVS) vientisumą ir brandą, įtvirtindama struktūruotą, rizika ir įrodymais grindžiamą audito bei stebėsenos praktiką.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 visiems vidaus verslo padaliniams, funkcijoms ir skyriams

2.1.2 fizinėms vietoms, debesijos aplinkoms, SaaS platformoms ir išorinėms paslaugoms

2.1.3 informacinėms sistemoms, taikomosioms programoms, infrastruktūrai ir duomenų ištekliams, kuriems taikoma ISVS

2.1.4 darbuotojams, rangovams ir trečiųjų šalių paslaugų teikėjams, kuriems taikomi audito ar atitikties reikalavimai

2.2 Politika apima:

2.2.1 vidaus auditus

2.2.2 išorės ir sertifikavimo auditus

2.2.3 techninę atitikties stebėseną

2.2.4 tiekėjų ir trečiųjų šalių auditus

2.2.5 korekcinius ir prevencinius veiksmus (CAPA)

2.2.6 rodiklius, suvestines ir ataskaitų teikimo procesus

2.3 Ji taikoma visoms organizacijai privalomoms aktualioms sistemoms ir standartams, įskaitant ISO/IEC 27001, ES BDAR, NIS2 direktyvą, DORA reglamentą, SOC 2 ir kitus.

3. Tikslai

3.1 Patikrinti įdiegtų kontrolės priemonių, politikų ir procedūrų tinkamumą bei veiksmingumą visoje ISVS ir susijusiose aplinkose.

3.2 Nustatyti ir pašalinti bet kokius trūkumus, neatitiktis ar atitikties spragas, kol jos neperaugo į incidentus ar pažeidimus.

3.3 Užtikrinti nuolatinį pasirengimą vidaus valdymo peržiūroms, išorės auditams ir nepriklausomam sertifikavimui.

3.4 Kaupti dokumentuotus įrodymus ir audito pėdsaką, reikalingus reguliavimo institucijų paklausimams, teisiniams procesams ar klientų patikinimo prašymams pagrįsti.

3.5 Integruoti audito rezultatus į platesnę organizacijos rizikos valdymo sistemą, saugumo rodiklius ir nuolatinio tobulinimo veiklą.

4. Vaidmenys ir atsakomybės

4.1 Vidaus audito vadovas / atitikties vadovas

4.1.1 planuoja, sudaro grafiką ir vykdo vidaus auditus pagal rizikos prioritetus

4.1.2 tvarko audito registrą, koordinuoja audito veiklą ir stebi korekcinių veiksmų įgyvendinimą

4.2 Informacijos saugumo vadovas (CISO)

4.2.1 užtikrina, kad audito taikymo sritis apimtų visus aktualius ISVS elementus ir A priedo kontrolės priemones

4.2.2 prižiūri CAPA tvirtinimą ir integruoja audito rezultatus į saugumo programą

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Šią politiką ne rečiau kaip kartą per metus turi peržiūrėti atitikties vadovas ir CISO arba anksčiau, jei įvyksta:

9.1.1 reguliacinių, sutartinių ar sertifikavimo sistemų pokyčiai

9.1.2 reikšmingos audito išvados arba pasikartojantys kontrolės priemonių nesuveikimo atvejai

9.1.3 organizacinės struktūros pertvarka arba GRC sistemos pokyčiai

9.1.4 išorės auditorių rekomendacijos arba reguliuotojų grįžtamasis ryšys

9.2 Peržiūros proceso metu turi būti įvertinama:

9.2.1 audito planavimo metodika ir dažnumas

9.2.2 ISVS taikymo srities arba infrastruktūros pokyčiai

9.2.3 kontrolės priemonių katalogo arba teisinių reikalavimų registro atnaujinimai

9.2.4 audito įrodymų ir CAPA procesų nuoseklumas bei kokybė

9.3 Visi politikos pakeitimai turi būti:

9.3.1 dokumentuoti saugykloje, valdomoje taikant versijų kontrolę

9.3.2 patvirtinti vadovybės

9.3.3 pranešti visam paveiktam personalui ir integruoti į atnaujintas procedūras bei informuotumo didinimo programas

9.4 Patvirtinimas po peržiūros turi užtikrinti, kad atnaujinti reikalavimai būtų atspindėti audito registre, atitikties priemonėse ir vidaus stebėsenos švieslentėse.

10. Susijusios politikos ir sąsajos

10.1 Ši politika derinama su šiomis susijusiomis organizacijos politikomis:

10.1.1 P1 – Informacijos saugumo politika: apibrėžia ISVS ir nustato atskaitomybę už atitiktį bei nuolatinį tobulinimą

10.1.2 P5 – Pakeitimų valdymo politika: užtikrina audito matomumą infrastruktūros ir konfigūracijų pakeitimams, darantiems poveikį kontrolės aplinkai

10.1.3 P6 – Rizikos valdymo politika: integruoja audito rezultatus į organizacijos rizikos vertinimo ir rizikos tvarkymo veiklą

10.1.4 P14 – Duomenų saugojimo ir sunaikinimo politika: reglamentuoja audito įrodymų, žurnalų ir atitikties įrašų saugojimą

10.1.5 P18 – Kriptografinių kontrolės priemonių politika: palaiko saugų jautrių audito duomenų saugojimą ir perdavimą

10.1.6 P26 – Trečiųjų šalių ir tiekėjų saugumo politika: apima audito teises, patikinimo dokumentaciją ir tiekėjų atitikties priežiūrą

10.1.7 P30 – Reagavimo į incidentus politika: suderina incidentų tvarkymo procesų auditus su ISVS patikinimo tikslais

10.1.8 P32 – Veiklos tęstinumo ir atkūrimo po katastrofos politika: reikalauja audito ciklų metu patikrinti veiklos tęstinumo testavimą ir DRP atitiktį

11. Pamatiniai standartai ir sistemos

11.1 Ši politika yra suderinta su pasauliniais audito ir nuolatinio atitikties patvirtinimo standartais bei teisiniais reikalavimais.

11.2 ISO/IEC 27001:

11.2.1 9.2 skyrius – vidaus auditas: reikalauja reguliarių, rizika grindžiamų ISVS auditų veiksmingumui ir atitikčiai įvertinti.

11.2.2 9.3 skyrius – vadovybės peržiūra: audito rezultatai turi būti įtraukiami į strateginę peržiūrą ir tobulinimą.

11.2.3 10.1 skyrius – neatitiktis ir korekciniai veiksmai: audito išvados turi būti tvarkomos pagal dokumentuotas CAPA procedūras.

11.3 ISO/IEC 27002:2022 – kontrolės priemonės 5.35–5.37:

11.3.1 A priedo kontrolės priemonės 5.35–5.37: apima nepriklausomą peržiūrą, teisinių ir sutartinių reikalavimų laikymąsi bei registravimą audito žurnale.

11.3.2 Jos pateikia įgyvendinimo gaires audito ir atitikties programų planavimui, vykdymui ir tobulinimui.

11.4 NIST SP 800-53 Rev.5:

11.4.1 CA-2 – kontrolės priemonių vertinimai: reikalauja reguliarios įdiegtų saugumo kontrolės priemonių peržiūros.

11.4.2 CA-5 – veiksmų planas ir etapai (POA&M): atitinka audito išvadų sekimą ir trūkumų šalinimą.

11.4.3 CA-7 – nuolatinė stebėsena: palaiko proaktyvius, automatizuotus atitikties vertinimus.

11.5 ES BDAR (2016/679):

11.5.1 24 ir 32 straipsniai: reikalauja turėti įrodymus apie saugumo kontrolės priemonių įgyvendinimą ir veiksmingumą taikant tinkamas valdymo struktūras.

11.5.2 33 straipsnis: pagrindžia poreikį turėti patvirtintą audito pėdsaką reaguojant į pažeidimus ir teikiant pranešimus.

11.6 ES NIS2 direktyva (2022/2555):

11.6.1 21 straipsnio 2 dalies g punktas: reikalauja atlikti politikų ir procedūrų auditą kaip minimalių kibernetinio saugumo rizikos valdymo priemonių dalį.

11.6.2 27 straipsnis: nacionalinės institucijos gali atlikti arba reikalauti auditų esminiams ir svarbiems subjektams.

11.7 ES DORA reglamentas (2022/2554):

11.7.1 10 straipsnio 2 dalies e punktas: subjektai turi atlikti IRT rizikos valdymo praktikos vidaus ir išorės auditus.

11.7.2 25 straipsnis – audito reikalavimai: nustato periodinių auditų, kuriuos atlieka vidaus arba nepriklausomi išorės auditoriai, reikalavimą, užtikrinant reguliacinį matomumą.

11.8 COBIT 2019:

11.8.1 MEA01 – veiksmingumo ir atitikties stebėjimas, vertinimas ir įvertinimas: užtikrina, kad kontrolės priemonių veiksmingumas būtų patikrintas ir apie jį būtų atsiskaitoma valdymo organams.

11.8.2 MEA03 – atitikties stebėjimas, vertinimas ir įvertinimas: reikalauja organizacijos praktikas suderinti su teisiniais, sutartiniais ir standartais grindžiamais reikalavimais.