					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P18					Dokumento pavadinimas: **Kriptografinių kontrolės priemonių 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	8 punktas	-
ISO/IEC 27002:2022	Kontrolės priemonės 8.24, 8.25, 8	-
NIST SP 800-53 Rev.5	SC-12–SC-17, SC-28, SC-28(1), SC-12(3)	-
ES BDAR	32 straipsnis, 33–34 straipsniai, 83 konstatuojamoji dalis	-
ES NIS2 direktyva	21 straipsnio 2 dalies d punktas	-
ES DORA reglamentas	6 straipsnio 2 dalies d punktas, 11 straipsnio 1 dalies c punktas	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Tikslas

1.1 Ši politika nustato privalomuosius reikalavimus saugiam ir atitiktį užtikrinančiam kriptografinių kontrolės priemonių naudojimui visoje organizacijoje, siekiant užtikrinti jautrios ir reguliuojamos informacijos konfidencialumą, vientisumą ir autentiškumą.

1.2 Kriptografijos naudojimas yra duomenų saugumo operacijų patikimumo pagrindas, palaiko saugų ryšį, užtikrina prieigos kontrolę ir leidžia laikytis reglamentavimo reikalavimų taikant veiksmingą šifravimą ir raktų valdymo praktiką.

1.3 Ši politika suderinta su ISO/IEC 27001:2022 8.1 punktu ir A priedo kontrole 8 bei 8.24, taip pat padeda vykdyti teisinius ir veiklos įpareigojimus pagal ES BDAR 32 straipsnį, DORA reglamento 6 straipsnio 2 dalies d punktą ir NIS2 direktyvos 21 straipsnį. Ji taip pat remia COBIT 2019 tikslus, susijusius su saugumo paslaugomis ir duomenų išteklių apsauga.

2. Taikymo sritis

2.1 Ši politika taikoma visiems organizacijos padaliniams, verslo funkcijoms, visam personalui ir trečiųjų šalių paslaugų teikėjams, dalyvaujantiems naudojant, administruojant ar diegiant kriptografines priemones ir metodus.

2.2 Apimamos gamybinės, kūrimo, parengiamosios, atsarginių kopijų ir atkūrimo po incidentų aplinkos sistemos, kuriose jautrūs duomenys perduodami, tvarkomi arba saugomi.

2.3 Taikymo sritis apima visus kriptografinius komponentus ir naudojimo atvejus, įskaitant, bet neapsiribojant:

2.3.1 simetriniu ir asimetriniu šifravimu

2.3.2 skaitmeniniais parašais ir sertifikatais

2.3.3 maišos algoritmais

2.3.4 saugiu raktų generavimu, paskirstymu ir sunaikinimu

2.3.5 Transport Layer Security (TLS), viso disko šifravimu (FDE) ir taikomųjų programų sąsajų lygmens šifravimu

2.3.6 saugiais komponentais, tokiais kaip Hardware Security Modules (HSM), Trusted Platform Modules (TPM) ir raktų valdymo sistemos (KMS)

2.4 Ši politika reglamentuoja kriptografijos naudojimą, susijusį su:

2.4.1 duomenimis, klasifikuojamais kaip Konfidencialūs, Labai konfidencialūs arba reguliuojami

2.4.2 autentifikavimu ir skaitmeninės tapatybės patvirtinimu

2.4.3 saugiu ryšiu su išorės šalimis

2.4.4 raktų saugojimo atsakomybe ir dvigubos kontrolės mechanizmais

3. Tikslai

3.1 Užtikrinti, kad kriptografinės technologijos būtų parenkamos, tvirtinamos, įgyvendinamos ir prižiūrimos pagal verslo riziką, tarptautinius standartus ir reglamentavimo reikalavimus.

3.2 Nustatyti standartizuotą valdysenos struktūrą kriptografinėms paslaugoms valdyti, aiškiai apibrėžiant atskaitomybę už įgyvendinimą, validavimą ir išimčių tvarkymą.

3.3 Užkirsti kelią neautorizuotam naudojimui, neteisingai konfigūracijai ar kriptografinių algoritmų ir kontrolės priemonių pasenimui taikant formalų tvirtinimo ir peržiūros procesą.

3.4 Užtikrinti, kad kriptografinės kontrolės priemonės būtų integruotos sistemų projektavimo etape ir reguliariai validuojamos, siekiant išvengti duomenų atskleidimo, raktų kompromitavimo ar protokolų susilpninimo.

3.5 Užtikrinti visų kriptografinių raktų gyvavimo ciklo valdymą, įskaitant generavimą, saugojimą, naudojimą, periodinį keitimą, atšaukimą ir saugų sunaikinimą.

3.6 Laikytis tarptautinių ir regioninių reglamentų, nustatančių šifravimo ir saugaus duomenų tvarkymo reikalavimus, įskaitant ES BDAR, DORA reglamentą, NIS2 direktyvą ir COBIT 2019.

4. Vaidmenys ir atsakomybės

4.1 Informacijos saugos vadovas / vyriausiasis informacijos saugumo pareigūnas

4.1.1 Valdo šią politiką ir užtikrina jos suderinamumą su informacijos saugumo valdymo sistema (ISVS) ir ISO/IEC 27001 A priedo kontrole 8.24.

4.1.2 Tvirtina kriptografinių algoritmų ir kontrolės priemonių naudojimą ir užtikrina politikos laikymąsi visoje organizacijoje.

4.2 Kriptografinių operacijų vadovas / saugumo architektas

4.2.1 Valdo kasdienę kriptografinių sistemų eksploatavimą ir administravimą.

4.2.2 Prižiūri patvirtintų kriptografinių metodų sąrašą (ACML) ir raktų valdymo registrą.

4.2.3 Atlieka kriptografinio projektavimo peržiūras (CDR) ir vertina naujas kriptografines technologijas.

[... 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 kasmet turi peržiūrėti informacijos saugos vadovas ir kriptografinių operacijų vadovas.

9.2 Peržiūros priežastys apima:

9.2.1 kriptografinių pažeidžiamumų nustatymą (pvz., algoritmo susilpninimą, kvantines atakas)

9.2.2 reglamentavimo pokyčius, reikalaujančius atnaujintų šifravimo standartų

9.2.3 veiklos arba audito išvadas, atskleidžiančias politikos spragas

9.2.4 kriptografinių priemonių atnaujinimus arba architektūrinius pakeitimus

9.3 Atnaujinimai turi būti valdomi pagal versijų kontrolę ISVS dokumentų kontrolės registre ir komunikuojami:

9.3.1 visiems administratoriams, turintiems kriptografinės prieigos vaidmenis

9.3.2 kūrimo komandoms ir DevSecOps vadovams

9.3.3 trečiųjų šalių teikėjams, kuriems taikomi sutartiniai šifravimo įpareigojimai

9.4 ISVS komanda turi užtikrinti, kad pakeistos versijos būtų archyvuojamos ir nebebūtų nurodomos veiklos procedūrose.

10. Susijusios politikos ir sąsajos

10.1 P1 - Informacijos saugumo politika. Nustato bazinę valdyseną visoms saugumo priemonėms, įskaitant kriptografinių kontrolės priemonių taikymą, turto apsaugą ir saugų ryšį.

10.2 P4 - Prieigos kontrolės politika. Užtikrina, kad loginė prieiga prie kriptografinės medžiagos ir šifravimo valdymo sistemų būtų griežtai ribojama pagal mažiausių privilegijų principą ir pareigų atskyrimą (SoD).

10.3 P6 - Rizikos valdymo politika. Palaiko kriptografinių kontrolės priemonių rizikų vertinimą ir dokumentuoja rizikos tvarkymo strategiją išimtims, algoritmų pasenimui arba raktų kompromitavimo scenarijams.

10.4 P12 - Turto valdymo politika. Nustato jautrių duomenų ir aparatinės įrangos turto klasifikavimo reikalavimą, kuris tiesiogiai lemia kriptografinius reikalavimus ir raktų saugojimo atsakomybę.

10.5 P13 - Duomenų klasifikavimo ir ženklinimo politika. Apibrėžia klasifikavimo lygius (pvz., Konfidencialūs, reguliuojami), kurie lemia konkrečius šifravimo reikalavimus perduodamiems ir saugomiems duomenims.

10.6 P14 - Duomenų saugojimo ir sunaikinimo politika. Nustato saugaus šifruotų saugojimo laikmenų ir kriptografinės raktų medžiagos sunaikinimo procedūras pasibaigus eksploatacijai.

10.7 P30 - Reagavimo į incidentus politika. Apibrėžia organizacijos reagavimo strategiją raktų kompromitavimo, netinkamo sertifikatų naudojimo arba įtariamų algoritminių pažeidžiamumų atvejais, įskaitant greitą atšaukimą ir pranešimą apie pažeidimus.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 punktas - Veiklos planavimas ir kontrolė: nustato technines saugumo kontrolės priemones, įskaitant kriptografines priemones, kaip veiklos apsaugos dalį.

11.2 ISO/IEC 27002:2022

11.2.1 Kontrolės priemonės 8.24, 8.25, 8: pateikia įgyvendinimo gaires dėl kriptografinių kontrolės priemonių tikslų, algoritmų parinkimo, protokolų taikymo ir sertifikatų gyvavimo ciklo valdymo.

11.3 NIST SP 800-53 Rev.

11.3.1 SC-12 - Kriptografinių raktų nustatymas: užtikrina saugų šifravimo raktų generavimą ir apsikeitimą jais. P18 nustato, kaip simetriniai ir asimetriniai raktai turi būti generuojami ir keičiami naudojant patvirtintus algoritmus ir protokolus.

11.3.2 SC-13 - Kriptografinė apsauga: nustato reikalavimą naudoti kriptografiją informacijos konfidencialumui ir vientisumui apsaugoti. P18 užtikrina šifravimą saugomiems ir perduodamiems duomenims pagal duomenų klasifikaciją, o algoritmų standartai derinami su NIST FIPS 140-3.

11.3.3 SC-17 - Viešojo rakto infrastruktūros (PKI) sertifikatai: reikalauja įgyvendinti PKI autentifikavimui ir skaitmeniniams parašams palaikyti. P18 apibrėžia PKI naudojimą ryšiui, sistemų tapatybėms ir administratoriaus lygmens prieigai apsaugoti.

11.3.4 SC-28, SC-28(1) - Informacijos apsauga saugant ir perduodant: reikalauja šifruoti duomenis, kai jie saugomi arba perduodami nepatikimais tinklais. P18 nustato TLS, VPN tunelių, viso disko šifravimo ir saugių saugojimo metodų taikymą jautriems duomenims.

11.3.5 SC-12(3) - Simetrinių raktų generavimas saugiam saugojimui ir paskirstymui: orientuota į saugų simetrinių raktų generavimą ir tvarkymą. P18 nustato reikalavimą naudoti stiprius atsitiktinių skaičių generatorius, raktų periodinio keitimo politiką ir saugias raktų saugyklas kriptografinėms operacijoms.

11.4 ES BDAR (2016/679)

11.4.1 32 straipsnis - Tvarkymo saugumas: aiškiai rekomenduoja šifravimą kaip asmens duomenų rizikos mažinimo priemonę.

11.4.2 83 konstatuojamoji dalis: pabrėžia šifravimą kaip kontrolės priemonę, padedančią išvengti neautorizuotos prieigos prie duomenų.

11.4.3 33 ir 34 straipsniai: jei šifravimas yra veiksmingas, organizacija tam tikrais atvejais gali būti atleista nuo pareigos pranešti apie pažeidimą.

11.5 ES NIS2 direktyva (2022/2555)

11.5.1 21 straipsnio 2 dalies d punktas: reikalauja techninių ir organizacinių priemonių, įskaitant kriptografines apsaugos priemones, paslaugų prieinamumui ir vientisumui palaikyti.

11.6 ES DORA reglamentas (2022/2554)

11.6.1 6 straipsnio 2 dalies d punktas: finansų įstaigos privalo apsaugoti duomenis, įskaitant stiprų kritinės informacijos šifravimą.

11.6.2 11 straipsnio 1 dalies c punktas: nustato saugaus duomenų tvarkymo kontrolės priemonių reikalavimą IRT trečiųjų šalių paslaugų teikėjams.

11.7 COBIT 2019

11.7.1 DSS05.01 - Informacijos išteklių apsauga: reikalauja naudoti šifravimą ir raktų valdymą siekiant apsaugoti duomenis nuo neautorizuotos prieigos.

11.7.2 DSS06.06 - Valdomas saugumo testavimas: rekomenduoja kriptografinės atitikties validavimą kaip pažeidžiamumų vertinimo dalį.

11.7.3 MEA03 - Atitikties stebėsena, vertinimas ir analizė: užtikrina nuolatinį kriptografinių kontrolės priemonių veiksmingumo patvirtinimą.