					Čia įrašykite registruoto juridinio asmens pavadinimą							
Dokumento numeris: P18S					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	Skyrius / straipsnis	Komentaras
ISO/IEC 27001:2022	8 skyrius	
ISO/IEC 27002:2022	Kontrolės priemonės 8.24, 8.25	
NIST SP 800-53 Rev.5	SC-12–SC-17	
ES NIS2 direktyva	21 straipsnio 2 dalies d, e punktai	
ES DORA reglamentas	6 straipsnio 2 dalies d punktas, 9 straipsnio 2 dalies f punktas	
COBIT 2019	DSS05.01, APO13	
ES BDAR	32 straipsnio 1 dalies a punktas, 34 straipsnis	

1. Tikslas

1.1 Ši politika nustato privalomuosius reikalavimus dėl šifravimo ir kriptografinių kontrolės priemonių naudojimo, siekiant apsaugoti veiklos duomenų ir asmens duomenų konfidencialumą, vientisumą ir autentiškumą.

1.2 Ji užtikrina, kad kriptografinės priemonės būtų tinkamai naudojamos MVĮ aplinkoje eksploatuojamose sistemose, įrenginiuose ir debesijos paslaugose.

1.3 Ši politika tiesiogiai prisideda prie ISO/IEC 27001:2022 sertifikavimo siekio ir padeda organizacijai vykdyti teisinius įsipareigojimus pagal ES Bendrąjį duomenų apsaugos reglamentą (BDAR), ES NIS2 direktyvą ir Skaitmeninio operacinio atsparumo aktą (DORA).

1.4 Šioje politikoje aptariamos kriptografinės kontrolės priemonės apima duomenų šifravimą, sertifikatų valdymą, saugų raktų valdymą ir šifruotas atsargines kopijas.

2. Taikymo sritis

2.1 Ši politika taikoma:

2.1.1 Visiems darbuotojams, rangovams ir trečiosioms šalims, tvarkančioms įmonės duomenis

2.1.2 Visoms veiklos sistemoms, galiniams įrenginiams ir debesijos platformoms, naudojamoms konfidencialiai informacijai saugoti, perduoti ar pasiekti

2.1.3 Visiems asmens, finansiniams, teisiniams ar jautriems įrašams, klasifikuojamiems pagal organizacijos duomenų klasifikavimo politiką

2.1.4 Visoms kriptografinėms kontrolės priemonėms, įskaitant šifravimo metodus, raktus, slaptažodžius, sertifikatus ir saugumo modulius

2.2 Politika apima saugomus, perduodamus ir naudojamus duomenis. Ji taip pat reglamentuoja šifravimą, taikomą atsarginėms kopijoms, el. paštui, išoriniams duomenų perdavimams ir viešosioms interneto svetainėms.

3. Tikslai

3.1 Užtikrinti, kad jautrūs ir reglamentuojami duomenys visada būtų apsaugoti tinkamomis kriptografinėmis priemonėmis

3.2 Apibrėžti atsakomybę už šifravimo priemonių parinkimą, konfigūravimą ir raktų valdymą

3.3 Užkirsti kelią neteisėtai prieigai, duomenų pakeitimui ar nutekėjimui, taikant saugaus perdavimo ir saugojimo kontrolės priemones

3.4 Laikytis teisinių ir reguliavimo reikalavimų, pagal kuriuos privaloma šifruoti asmens ir veiklos duomenis

3.5 Palaikyti veiklos saugumą ir prieinamumą veiksmingai valdant sertifikatus ir kriptografinius raktus

4. Vaidmenys ir atsakomybės

4.1 Generalinis vadovas (GV)

4.1.1 Tvirtina šią politiką ir užtikrina, kad kriptografiniai reikalavimai būtų įgyvendinami

4.1.2 Peržiūri išimtis, pranešimus apie pažeidimus ir tiekėjų atitiktį šifravimo reikalavimams

4.1.3 Patvirtina, kad išorinės arba debesijos paslaugos atitinka šifravimo standartus

4.2 IT paslaugų teikėjas / vidaus IT administratorius

4.2.1 Įgyvendina ir prižiūri šifravimo sprendimus (pvz., viso disko šifravimą, SSL sertifikatus, VPN)

4.2.2 Valdo kriptografinių raktų gyvavimo ciklą ir saugaus saugojimo priemones

4.2.3 Konfigūruoja ir stebi šifravimą, taikomą atsarginių kopijų, interneto svetainių ir įrenginių apsaugai

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

9. Peržiūros ir atnaujinimo reikalavimai

9.1 Metinė peržiūra

9.1.1 Ši politika turi būti peržiūrima ne rečiau kaip kartą per metus generalinio vadovo, koordinuojant veiksmus su IT paslaugų teikėju ir privatumo koordinatoriumi.

9.2 Tarpinių peržiūrų inicijavimo atvejai

9.2.1 Peržiūros taip pat turi būti atliekamos, jei:

9.2.1.1 Pasikeičia kriptografijos standartai ar protokolai (pvz., algoritmas tampa nebenaudotinas)

9.2.1.2 Įdiegiamos naujos sistemos arba debesijos paslaugos

9.2.1.3 Įvyksta pažeidimas ar incidentas, susijęs su kompromituotu raktu arba sertifikatu

9.2.1.4 Teisiniai ar reguliavimo pakeitimai turi įtakos šifravimo reikalavimams

9.3 Versijų kontrolė ir komunikacija

9.3.1 Visi politikos pakeitimai turi būti dokumentuojami versijų kontrolės žurnale

9.3.2 Darbuotojai turi būti informuojami apie atnaujinimus, o ankstesnės versijos archyvuojamos

9.3.3 Naujausia patvirtinta versija turi būti saugoma centrinėje politikų saugykloje

10. Susijusios politikos ir sąsajos

10.1 Ši politika turi būti taikoma kartu su šiomis MVĮ politikomis:

10.1.1 P12S – Turto valdymo politika: užtikrina, kad šifravimas būtų taikomas klasifikuotiems ištekliams jų saugojimo, perdavimo ir sunaikinimo metu.

10.1.2 P14S – Duomenų saugojimo ir sunaikinimo politika: apibrėžia saugojimo laikotarpius ir reikalauja šifruoto duomenų saugojimo iki jų saugaus sunaikinimo.

10.1.3 P17S – Duomenų apsaugos ir privatumo politika: suderina šifravimą su duomenų apsaugos principais ir reguliavimo lūkesčiais pagal BDAR 32 straipsnį.

10.1.4 P22S – Žurnalų tvarkymo ir stebėsenos politika: reikalauja audito tikslais registruoti raktų naudojimą, šifravimo sutrikimus ir sertifikatų galiojimo pabaigą.

10.1.5 P30S – Reagavimo į incidentus politika: nustato eskalavimo, lokalizavimo ir pranešimo procedūras, kai šifravimas neveikia arba raktai yra kompromituoti.

11. Pamatiniai standartai ir sistemos

11.1 ISO/IEC 27001

11.1.1 8.1 skyrius – reikalauja įgyvendinti operacines kontrolės priemones, įskaitant šifravimą, siekiant valdyti saugumo rizikas.

11.2 ISO/IEC 27002

11.2.1 Kontrolės priemonė 8.24 – aprašo reikalavimus dėl šifravimo taikymo konfidencialumui ir vientisumui užtikrinti.

11.2.2 Kontrolės priemonė 8.25 – nustato saugaus kriptografinių raktų ir sertifikatų valdymo reikalavimus.

11.3 NIST SP 800-53 Rev.5

11.3.1 SC-12 – nustato kriptografinių raktų sukūrimo ir validavimo reikalavimus.

11.3.2 SC-13 – apibrėžia kriptografinių raktų generavimo standartus.

11.3.3 SC-17 – apima viešojo rakto infrastruktūrą (PKI) ir sertifikatų gyvavimo ciklo valdymą.

11.3.4 SC-28 – reikalauja saugomų duomenų šifravimo.

11.3.5 SC-12–SC-17 (šeima) – užtikrina, kad kriptografinės apsaugos priemonės būtų tinkamai įgyvendintos visose sistemose.

11.4 ES BDAR

11.4.1 32 straipsnio 1 dalies a punktas – reikalauja, kad organizacijos įgyvendintų technines priemones, tokias kaip šifravimas, duomenų konfidencialumui užtikrinti.

11.4.2 34 straipsnis – numato, kad šifravimas gali atleisti organizaciją nuo pareigos pranešti apie pažeidimą, jei duomenys buvo nesuprantami neįgaliotiems asmenims.

11.5 ES NIS2 direktyva

11.5.1 21 straipsnio 2 dalies d punktas – reikalauja taikyti veiksmingą šifravimą sistemoms ir ryšiams apsaugoti.

11.5.2 21 straipsnio 2 dalies e punktas – pabrėžia duomenų apsaugą ir kibernetinių grėsmių mažinimą taikant šifravimą.

11.6 ES DORA reglamentas

11.6.1 6 straipsnio 2 dalies d punktas – reikalauja, kad IRT sistemos palaikytų saugius ryšio kanalus ir šifravimą.

11.6.2 9 straipsnio 2 dalies f punktas – įpareigoja finansų subjektus naudoti stiprų šifravimą skaitmeniniams ryšiams ir duomenų mainams apsaugoti.

11.7 COBIT 2019

11.7.1 DSS05.01 – nustato reikalavimą apsaugoti jautrią informaciją taikant šifravimą ir kriptografinius protokolus.

11.7.2 APO13.02 – reikalauja veiksmingai įgyvendinti saugumo kontrolės priemones, įskaitant kriptografines apsaugos priemones, kaip informacijos saugumo planavimo dalį.