					Čia įrašykite registruoto juridinio asmens pavadinimą						
Dokumento numeris: P38					Dokumento pavadinimas: **Saugios komunikacijos ir kelių veiksnių autentifikavimo 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	Pastaba
ISO/IEC 27001:2022	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
ES BDAR	32 straipsnio 1 dalies b punktas	
ES NIS2 direktyva	21 straipsnio 2 dalies j punktas	
ES DORA reglamentas	9 straipsnio 2 dalies d punktas, 11 straipsnis	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Tikslas

1.1 Nustatyti reikalavimus, taikomus kelių veiksnių autentifikavimo (MFA) arba tęstinio autentifikavimo sprendimų naudojimui, suteikiant prieigą prie sistemų, laikantis ES NIS2 direktyvos 21 straipsnio 2 dalies j punkto.

1.2 Nustatyti apsaugos priemones saugiems balso, vaizdo, tekstiniams ir avariniams ryšiams, siekiant užtikrinti informacijos konfidencialumą ir vientisumą.

2. Taikymo sritis

2.1 Ši politika taikoma visiems organizacijoje naudojamiems autentifikavimo mechanizmams ir ryšių sistemoms (balso skambučiams, vaizdo konferencijoms, žinučių siuntimui ir avarinio pranešimo sistemoms).

2.2 Ji apima visus darbuotojus, rangovus ir visas išorės šalis, kurios naudojasi organizacijos ryšių kanalais arba gauna prieigą prie jos tinklo ir informacinių sistemų.

3. Tikslai

3.1 Užtikrinti, kad prieiga prie sistemų būtų suteikiama tik tinkamai autentifikuotiems naudotojams, mažinant neteisėtos prieigos riziką, įgyvendinus kelių veiksnių autentifikavimą (MFA).

3.2 Užtikrinti, kad vidaus ir avariniai ryšiai būtų perduodami saugiais būdais (pvz., naudojant šifruotus kanalus), taip užkertant kelią pasiklausymui ar klastojimui.

3.3 Užtikrinti atitiktį ES NIS2 direktyvos reikalavimams dėl stipraus autentifikavimo ir saugių ryšių, stiprinant bendrą kibernetinį atsparumą.

4. Vaidmenys ir atsakomybės

4.1 Vyriausiasis informacijos saugumo pareigūnas / IT saugumo funkcija: nustato ir prižiūri kelių veiksnių autentifikavimo (MFA) mechanizmus ir saugių ryšių priemones; užtikrina techninį šios politikos įgyvendinimą.

4.2 IT administratoriai: įgyvendina kelių veiksnių autentifikavimą (MFA) atitinkamose sistemose ir sukonfigūruoja patvirtintas saugių ryšių platformas; vykdo atitikties stebėseną.

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

9. Stebėsena ir auditas

9.1 IT saugumo funkcija turi nuolat vykdyti autentifikavimo žurnalų stebėseną, siekdama nustatyti vieno veiksnio prisijungimo bandymus arba anomalijas, susijusias su kelių veiksnių autentifikavimo (MFA) nesėkmėmis. Saugių ryšių sistemų žurnalai (kai taikoma) taip pat turi būti stebimi siekiant nustatyti neteisėtos prieigos bandymus arba konfigūracijos pakeitimus.

9.2 Vidaus audito funkcija kasmet peržiūri kelių veiksnių autentifikavimo (MFA) diegimo atitiktį (užtikrindama, kad visose kritinėse sistemose būtų taikomas kelių veiksnių autentifikavimas (MFA)) ir patikrina, kad jautriems ryšiams būtų naudojami tik patvirtinti saugūs kanalai. Audito išvados pateikiamos vadovybei kartu su rekomendacijomis.

10. Peržiūra ir priežiūra

10.1 Ši politika peržiūrima ne rečiau kaip kartą per metus, taip pat po bet kurio reikšmingo saugumo incidento arba nustačius naują su autentifikavimu ar ryšiais susijusią riziką (pvz., naujus grėsmių vektorius prieš kelių veiksnių autentifikavimą (MFA) arba nesaugių ryšių naudojimo atvejus).

10.2 Prireikus atliekami pakeitimai, siekiant atsižvelgti į technologijų raidą (pvz., patikimesnių tęstinio autentifikavimo sprendimų diegimą) arba laikytis atnaujintų reguliavimo gairių (pvz., būsimų ENISA rekomendacijų dėl saugių ryšių).

11. Susijusios politikos ir sąsajos

11.1 P01 – Informacijos saugumo politika. Nustato visos organizacijos mastu taikomas autentifikavimo ir ryšių apsaugos priemones.

11.2 P04 – Prieigos kontrolės politika. Nustato prieigos valdyseną, kurią P38 politika įgyvendina taikydama kelių veiksnių autentifikavimą (MFA).

11.3 P11 – Naudotojų paskyrų ir privilegijų valdymo politika. Susieja kelių veiksnių autentifikavimą (MFA) su privilegijuotosios prieigos gyvavimo ciklu.

11.4 P18 – Kriptografinių kontrolės priemonių politika. Nustato patvirtintus kriptografijos ir raktų valdymo reikalavimus saugiems ryšiams.

11.5 P21 – Tinklo saugumo politika. Apsaugo balso, vaizdo ir žinučių perdavimui naudojamus perdavimo kanalus.

11.6 P22 – Žurnalų tvarkymo ir stebėsenos politika. Užtikrina autentifikavimo įvykių ir saugių kanalų naudojimo stebėseną.

11.7 P32 – Veiklos tęstinumo ir atkūrimo po katastrofos politika. Užtikrina avarinių ryšių saugumą krizės metu.

11.8 P08 – Informacijos saugumo supratimo ir mokymo politika. Nustato naudotojų mokymą apie kelių veiksnių autentifikavimą (MFA) ir ryšių kanalų higieną.

12. Nuorodos

12.1 NIS2 direktyva (ES 2022/2555), 21 straipsnio 2 dalies j punktas (kelių veiksnių autentifikavimo ir saugių ryšių naudojimas)

12.2 Komisijos įgyvendinimo reglamentas (ES) 2024/2690, priedo 11 skyrius (prieigos kontrolės reikalavimai, įskaitant kelių veiksnių autentifikavimą (MFA) privilegijuotosioms paskyroms)

12.3 ISO/IEC 27001:2022 ir ISO/IEC 27002: