					Ovdje unesite naziv registrirane pravne osobe							
Broj dokumenta: P38					Naziv dokumenta: **Politika sigurnih komunikacija i višefaktorske autentifikacije**							
Verzija: 1.0		Datum stupanja na snagu: 01.01.2025			Vlasnik dokumenta:							
X	Politika		Standard		Postupak		Obrazac		Registar		Drugo	

Povijest revizija				
Broj revizije	**Datum revizije**	**Promjene**	**Pregledao/la**	**Vlasnik procesa**

Odobrenja			
Ime	**Radno mjesto**	**Datum**	**Potpis**

Usklađeno sa standardima i propisima

Standard/regulativa	Točka/članak	Napomena
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	
GDPR EU	čl. 32. st. 1. t. b	
Direktiva EU NIS2	čl. 21. st. 2. t. j	
Uredba EU DORA	čl. 9. st. 2. t. d, čl. 11.	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Svrha

1.1 Ovom politikom utvrđuju se zahtjevi za primjenu višefaktorske ili kontinuirane autentikacije pri pristupu sustavima, u skladu s člankom 21. stavkom 2. točkom (j) Direktive EU NIS2.

1.2 Ovom politikom uspostavljaju se kontrole za sigurne glasovne, videokomunikacijske, tekstualne i hitne komunikacije radi zaštite povjerljivosti i cjelovitosti informacija.

2. Područje primjene

2.1 Ova politika primjenjuje se na sve mehanizme autentikacije i komunikacijske sustave (glasovni pozivi, videokonferencije, razmjena poruka i sustavi za hitno obavještavanje) koje organizacija koristi.

2.2 Ova politika obuhvaća sve zaposlenike, ugovorne izvršitelje i sve vanjske strane koje koriste komunikacijske kanale organizacije ili pristupaju njezinim mrežnim i informacijskim sustavima.

3. Ciljevi

3.1 Osigurati da pristup sustavima ostvaruju samo primjereno autentikirani korisnici, uz smanjenje rizika od neovlaštenog pristupa primjenom MFA-a.

3.2 Osigurati da se interne i hitne komunikacije prenose sigurnim metodama (npr. kriptiranim kanalima) kako bi se spriječilo prisluškivanje ili neovlaštena izmjena.

3.3 Osigurati usklađenost sa zahtjevima Direktive EU NIS2 za snažnu autentikaciju i sigurne komunikacije te ojačati ukupnu kibernetičku otpornost.

4. Uloge i odgovornosti

4.1 CISO / funkcija informacijske sigurnosti: utvrđuje i održava MFA mehanizme i alate za sigurne komunikacije te osigurava tehničku provedbu ove politike.

4.2 IT administratori: provode MFA za relevantne sustave, konfiguriraju odobrene platforme za sigurne komunikacije i prate usklađenost.

[... Odjeljci 4.3–8 nisu uključeni u ovaj pregled. Kupite cijeli dokument za pristup potpunom sadržaju. ...]

9. Praćenje i revizija

9.1 Funkcija informacijske sigurnosti mora kontinuirano pratiti zapise dnevnika autentikacije radi otkrivanja pokušaja prijave samo jednim faktorom ili neuobičajenih MFA neuspjeha. Zapisi dnevnika sustava za sigurne komunikacije, gdje je primjenjivo, moraju se pratiti radi otkrivanja pokušaja neovlaštenog pristupa ili promjena konfiguracije.

9.2 Interna revizija jednom godišnje pregledava usklađenost sa zahtjevima za uvođenje MFA-a, uključujući provjeru da svi kritični sustavi zahtijevaju MFA, te potvrđuje da se za osjetljive komunikacije koriste isključivo odobreni sigurni kanali. Nalazi se dostavljaju upravi zajedno s preporukama.

10. Pregled i održavanje

10.1 Ova politika pregledava se najmanje jednom godišnje te nakon svakog većeg sigurnosnog incidenta ili novoutvrđenog rizika povezanog s autentikacijom ili komunikacijama (npr. novi vektori prijetnji usmjereni na MFA ili otkrivanje uporabe nesigurnih komunikacijskih kanala).

10.2 Izmjene se provode prema potrebi radi odgovora na razvoj tehnologije (npr. uvođenje robusnijih rješenja kontinuirane autentikacije) ili radi usklađenosti s ažuriranim regulatornim smjernicama (kao što su buduće preporuke ENISA-e o sigurnim komunikacijama).

11. Povezane politike i upućivanja

11.1 P01 – Politika informacijske sigurnosti. Propisuje zaštitne mjere za autentikaciju i komunikacije na razini cijele organizacije.

11.2 P04 – Politika upravljanja pristupom. Uspostavlja okvir upravljanja pristupom koji se u politici P38 nadopunjuje zahtjevima za MFA.

11.3 P11 – Politika upravljanja korisničkim računima i ovlastima. Povezuje MFA sa životnim ciklusom povlaštenog pristupa.

11.4 P18 – Politika kriptografskih kontrola. Propisuje odobrene kriptografske mehanizme i upravljanje ključevima za sigurne komunikacije.

11.5 P21 – Politika mrežne sigurnosti. Štiti prijenosne kanale koji se koriste za glasovne, videokomunikacijske i tekstualne usluge.

11.6 P22 – Politika zapisivanja i praćenja. Uređuje praćenje autentikacijskih događaja i uporabe sigurnih kanala.

11.7 P32 – Politika neprekidnosti poslovanja i oporavka od katastrofe. Uređuje sigurnost hitnih komunikacija tijekom kriznih situacija.

11.8 P08 – Politika podizanja svijesti i osposobljavanja za informacijsku sigurnost. Osposobljava korisnike za MFA i sigurno korištenje komunikacijskih kanala.

12. Reference

12.1 Direktiva NIS2 (EU 2022/2555), članak 21. stavak 2. točka (j) (uporaba višefaktorske autentikacije i sigurnih komunikacija)

12.2 Provedbena uredba Komisije (EU) 2024/2690, Prilog, odjeljak 11. (zahtjevi za upravljanje pristupom, uključujući MFA za povlaštene račune)

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