					Sem vnesite naziv registrirane pravne osebe							
Številka dokumenta: P38					Naslov dokumenta: **Politika varnih komunikacij in večfaktorske avtentikacije**							
Različica: 1.0		Datum začetka veljavnosti: 01.01.2025			Lastnik dokumenta:							
X	Politika		Standard		Postopek		Obrazec		Register		Drugo	

Zgodovina revizij				
Številka revizije	**Datum revizije**	**Spremembe**	**Pregledal**	**Lastnik procesa**

Odobritve			
Ime	**Delovno mesto**	**Datum**	**Podpis**

Usklajenost s standardi in predpisi

Standard/predpis	Klavzula/člen	Komentar
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	
Uredba EU GDPR	člen 32(1)(b)	
Direktiva EU NIS2	člen 21(2)(j)	
Uredba EU DORA	člen 9(2)(d), člen 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05	

1. Namen

1.1 Določiti zahteve za uporabo večfaktorske avtentikacije (MFA) ali rešitev za neprekinjeno avtentikacijo pri dostopu do sistemov v skladu s členom 21(2)(j) Direktive EU NIS2.

1.2 Določiti kontrole za varne glasovne, video-, besedilne komunikacije in komunikacije v sili za zaščito celovitosti in zaupnosti informacij.

2. Področje uporabe

2.1 Ta politika se uporablja za vse avtentikacijske mehanizme in komunikacijske sisteme (glasovne klice, videokonferenčne rešitve, sporočanje in sisteme za obveščanje v sili), ki jih uporablja organizacija.

2.2 Velja za vse zaposlene, pogodbene izvajalce in vse zunanje strani, ki uporabljajo komunikacijske kanale organizacije ali dostopajo do njenih omrežnih in informacijskih sistemov.

3. Cilji

3.1 Zagotoviti, da dostop do sistemov pridobijo samo ustrezno avtenticirani uporabniki, ter z uvedbo večfaktorske avtentikacije (MFA) zmanjšati tveganje nepooblaščenega dostopa.

3.2 Zagotoviti, da se notranje komunikacije in komunikacije v sili prenašajo z uporabo varnih metod (npr. šifriranih kanalov), s čimer se preprečita prisluškovanje in nedovoljeni posegi.

3.3 Zagotoviti skladnost z zahtevami Direktive EU NIS2 glede močne avtentikacije in varnih komunikacij ter s tem okrepiti splošno kibernetsko odpornost.

4. Vloge in odgovornosti

4.1 Vodja informacijske varnosti (CISO) / funkcija informacijske varnosti IT: opredeli in vzdržuje mehanizme večfaktorske avtentikacije (MFA) ter orodja za varne komunikacije in zagotavlja tehnično uveljavitev te politike.

4.2 Skrbniki IT: uvedejo večfaktorsko avtentikacijo (MFA) za ustrezne sisteme in konfigurirajo odobrene platforme za varne komunikacije ter spremljajo skladnost.

[... Razdelki 4.3–8 niso vključeni v ta predogled. Kupite celoten dokument za dostop do celotne vsebine. ...]

9. Spremljanje in presoja

9.1 Funkcija informacijske varnosti IT mora stalno spremljati dnevnike avtentikacije zaradi poskusov prijave z enim samim faktorjem, anomalij pri prijavah ali nenavadnih neuspešnih poskusov MFA.

Dnevniki sistemov za varne komunikacije se, kjer je to primerno, spremljajo zaradi poskusov nepooblaščenega dostopa ali sprememb konfiguracije.

9.2 Notranja revizija letno pregleda skladnost uvedbe večfaktorske avtentikacije (MFA), da se zagotovi, da vsi kritični sistemi uveljavljajo MFA, ter preveri, da se za občutljive komunikacije uporabljajo izključno odobreni varni kanali. Ugotovitve presoje se posredujejo vodstvu skupaj s priporočili.

10. Pregled in vzdrževanje

10.1 Ta politika se pregleda najmanj enkrat letno ter ob vsakem večjem varnostnem incidentu ali na novo ugotovljenem tveganju, povezanem z avtentikacijo ali komunikacijami (npr. novi vektorji groženj proti MFA ali ugotovljena uporaba nevarnih komunikacijskih kanalov).

10.2 Po potrebi se izvedejo spremembe za obravnavo razvoja tehnologij (npr. uvedba robustnejših rešitev za neprekinjeno avtentikacijo) ali za zagotovitev skladnosti s posodobljenimi regulativnimi smernicami (kot so prihodnja priporočila agencije ENISA glede varnih komunikacij).

11. Povezane politike in povezave

11.1 P01 – Politika informacijske varnosti. Določa zaščitne ukrepe za avtentikacijo in komunikacije na ravni celotne organizacije.

11.2 P04 – Politika nadzora dostopa. Vzpostavlja upravljanje pravic dostopa, ki ga MFA v P38 uveljavlja.

11.3 P11 – Politika upravljanja uporabniških računov in privilegijev. Povezuje MFA z življenjskim ciklom privilegiranega dostopa.

11.4 P18 – Politika kriptografskih kontrol. Določa odobrena kriptografska orodja in metode ter upravljanje ključev za varne komunikacije.

11.5 P21 – Politika varnosti omrežja. Varuje prenosne poti, ki se uporabljajo za glasovne, video- in sporočilne storitve.

11.6 P22 – Politika beleženja in spremljanja. Spremlja dogodke avtentikacije in uporabo varnih kanalov.

11.7 P32 – Politika neprekinjenega poslovanja in obnovitve po nesreči. Varuje komunikacije v sili med kriznimi dogodki.

11.8 P08 – Politika ozaveščanja in usposabljanja za informacijsko varnost. Uporabnike usposablja za MFA in varno uporabo komunikacijskih kanalov.

12. Reference

12.1 Direktiva NIS2 (EU 2022/2555), člen 21(2), točka (j) (uporaba večfaktorske avtentikacije in varnih komunikacij)

12.2 Izvedbena uredba Komisije (EU) 2024/2690, Priloga, oddelek 11 (zahteve glede nadzora dostopa, vključno z MFA za privilegirane račune)

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