					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P38					Titlul documentului: **Politica privind comunicațiile securizate și autentificarea multifactor**							
Versiunea: 1.0		Data intrării în vigoare: 01.01.2025			Proprietarul documentului:							
X	Politică		Standard		Procedură		Formular		Registru		Altul	

Istoricul reviziilor				
Numărul reviziei	**Data reviziei**	**Modificări**	**Revizuit de**	**Proprietarul procesului**

Aprobări			
Nume	**Funcție**	**Data**	**Semnătură**

Aliniată la standardele și reglementările aplicabile

Standard/reglementare	Clauză/articol	Comentariu
ISO/IEC 27001:2022	5.30, 5.31, 8.24	
ISO/IEC 27002:2022	5.15, 5.17, 5.18, 8.24, 8.28	
RGPD al UE	Art. 32(1)(b)	
NIST SP 800-53 Rev.5	IA-2, IA-3, IA-5, IA-8, SC-12, SC-13, SC-31	
Directiva NIS2 a UE	Art. 21(2)(j)	
Regulamentul DORA al UE	Art. 9(2)(d), Art. 11	
COBIT 2019	DSS05.04, DSS05.05, DSS05.	

1. Scop

1.1 Definește cerințele pentru utilizarea soluțiilor de autentificare multifactor sau de autentificare continuă pentru accesul la sisteme, în conformitate cu articolul 21 alineatul (2) litera (j) din Directiva NIS2 a UE.

1.2 Stabilește controale pentru comunicațiile securizate de voce, video, text și de urgență, pentru a proteja confidențialitatea și integritatea informațiilor.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor mecanismelor de autentificare și sistemelor de comunicații (apeluri vocale, videoconferințe, mesagerie și sisteme de notificare de urgență) utilizate de organizație.

2.2 Aceasta se aplică tuturor angajaților, contractorilor și oricăror terți care utilizează canalele de comunicații ale organizației sau accesează rețelele și sistemele sale informatice și de informații.

3. Obiective

3.1 Asigură că numai utilizatorii autentificați în mod corespunzător obțin acces la sisteme, reducând riscul de acces neautorizat prin implementarea autentificării multifactor.

3.2 Asigură că comunicațiile interne și cele de urgență sunt transmise prin metode securizate (de exemplu, canale criptate), prevenind interceptarea sau alterarea.

3.3 Asigură conformitatea cu cerințele NIS2 privind autentificarea puternică și comunicațiile securizate, consolidând nivelul general de reziliență cibernetică.

4. Roluri și responsabilități

4.1 Directorul pentru securitatea informațiilor / echipa de securitate a informațiilor: definesc și mențin mecanismele de autentificare multifactor și instrumentele de comunicații securizate; asigură implementarea tehnică a prezentei politici.

4.2 Administratorii de sistem: implementează autentificarea multifactor pentru sistemele relevante și configurează platformele aprobate pentru comunicații securizate; monitorizează conformitatea.

[... Secțiunile 4.3–8 nu sunt incluse în această previzualizare. Achiziționați documentul complet pentru a accesa conținutul integral. ...]

9. Monitorizare și audit

9.1 Echipa de securitate a informațiilor trebuie să monitorizeze continuu jurnalele de autentificare pentru orice tentative de autentificare cu un singur factor sau pentru eșecuri anormale ale autentificării

multifactor. Jurnalele sistemelor de comunicații securizate (acolo unde este cazul) trebuie monitorizate pentru tentative de acces neautorizat sau modificări de configurație.

9.2 Auditul Intern va revizui anual respectarea cerințelor privind implementarea autentificării multifactor (asigurând că toate sistemele critice impun autentificarea multifactor) și va verifica utilizarea exclusivă a canalelor securizate aprobate pentru comunicațiile sensibile. Constatările vor fi raportate managementului împreună cu recomandări.

10. Revizuire și mentenanță

10.1 Această politică va fi revizuită cel puțin anual și în urma oricărui incident major de securitate sau a oricărui risc nou identificat legat de autentificare sau comunicații (de exemplu, noi vectori de amenințare împotriva autentificării multifactor, identificarea utilizării unor comunicații nesecurizate).

10.2 Revizuirile vor fi efectuate ori de câte ori este necesar pentru a răspunde evoluției tehnologiilor (de exemplu, adoptarea unor soluții mai robuste de autentificare continuă) sau pentru a asigura conformitatea cu orientările de reglementare actualizate (cum ar fi viitoare recomandări ENISA privind comunicațiile securizate).

11. Politici conexe și interdependențe

11.1 P01 – Politica de securitate a informației. Impune măsuri de protecție la nivelul întregii organizații pentru autentificare și comunicații.

11.2 P04 – Politica de control al accesului. Stabilește guvernanța accesului, pe care autentificarea multifactor din P38 o pune în aplicare.

11.3 P11 – Politica privind gestionarea conturilor de utilizator și a privilegiilor. Corelează autentificarea multifactor cu ciclul de viață al accesului privilegiat.

11.4 P18 – Politica privind controalele criptografice. Oferă mecanismele criptografice aprobate și procesele de management al cheilor pentru comunicații securizate.

11.5 P21 – Politica de securitate a rețelei. Securizează canalele de transport utilizate pentru voce/video/mesagerie.

11.6 P22 – Politica de jurnalizare și monitorizare. Monitorizează evenimentele de autentificare și utilizarea canalelor securizate.

11.7 P32 – Politica privind continuitatea activității și recuperarea în caz de dezastru. Securizează comunicațiile de urgență în timpul situațiilor de criză.

11.8 P08 – Politica privind conștientizarea și instruirea în domeniul securității informației. Instruiește utilizatorii privind autentificarea multifactor și utilizarea corectă a canalelor.

12. Referințe

12.1 Directiva NIS2 (UE 2022/2555), articolul 21 alineatul (2), litera (j) (utilizarea autentificării multifactor și a comunicațiilor securizate)

12.2 Regulamentul de punere în aplicare al Comisiei (UE) 2024/2690, secțiunea 11 din anexă (cerințe privind controlul accesului, inclusiv autentificarea multifactor pentru conturile privilegiate)

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