					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P18					Titlul documentului: **Politica privind controalele criptografice**							
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	Clauza 8	-
ISO/IEC 27002:2022	Controalele 8.24, 8.25, 8	-
NIST SP 800-53 Rev. 5	SC-12 până la SC-17, SC-28, SC-28(1), SC-12(3)	-
GDPR UE	Articolul 32, articolele 33-34, considerentul 83	-
Directiva UE NIS2	Articolul 21(2)(d)	-
Regulamentul UE DORA	Articolele 6(2)(d), 11(1)(c)	-
COBIT 2019	DSS05.01, DSS06.06, MEA	-

1. Scop

1.1 Această politică stabilește cerințele obligatorii pentru utilizarea sigură și conformă a controalelor criptografice la nivelul întregii organizații, pentru a asigura confidențialitatea, integritatea și autenticitatea informațiilor sensibile și reglementate.

1.2 Utilizarea criptografiei stă la baza încrederii în activitățile de securitate a datelor, susține comunicațiile securizate, aplicarea controlului accesului și conformitatea cu cerințele de reglementare prin practici eficace de criptare și de management al cheilor.

1.3 Această politică este aliniată cu ISO/IEC 27001:2022, Clauza 8.1 și Anexa A, Controlul 8.24, și susține obligațiile legale și operaționale prevăzute la articolul 32 din GDPR, articolul 6(2)(d) din DORA și articolul 21 din NIS2. De asemenea, susține obiectivele COBIT 2019 privind serviciile de securitate și protecția activelor informaționale.

2. Domeniu de aplicare

2.1 Această politică se aplică tuturor unităților organizaționale, funcțiilor de business, întregului personal și furnizorilor terți de servicii implicați în utilizarea, administrarea sau implementarea instrumentelor și metodelor criptografice.

2.2 Mediile acoperite includ sistemele de producție, dezvoltare, testare intermediară, backup și recuperare în caz de dezastru în care datele sensibile sunt transmise, prelucrate sau stocate.

2.3 Domeniul de aplicare include toate componentele criptografice și toate cazurile de utilizare, inclusiv, fără a se limita la:

2.3.1 criptare simetrică și asimetrică

2.3.2 semnături digitale și certificate

2.3.3 algoritmi de hash

2.3.4 generarea, distribuirea și distrugerea securizată a cheilor

2.3.5 Transport Layer Security (TLS), criptarea completă a discului (FDE) și criptarea la nivel de API

2.3.6 elemente securizate, precum module hardware de securitate (HSM), module de platformă de încredere (TPM) și sisteme de management al cheilor (KMS)

2.4 Această politică reglementează utilizarea criptografiei în raport cu:

2.4.1 date clasificate ca Confidențial, Strict confidențial sau Reglementat

2.4.2 autentificarea și verificarea identității digitale

2.4.3 comunicațiile securizate cu părți externe

2.4.4 custodia cheilor și mecanismele de control dual

3. Obiective

3.1 Să asigure că tehnologiile criptografice sunt selectate, aprobate, implementate și menținute în conformitate cu riscul de business, standardele internaționale și cerințele de reglementare.

3.2 Să stabilească o structură de guvernanță standardizată pentru administrarea serviciilor criptografice, incluzând responsabilități clare pentru implementare, validare și gestionarea excepțiilor.

3.3 Să prevină utilizarea neautorizată, configurarea eronată sau învechirea algoritmilor și controalelor criptografice printr-un proces formal de aprobare și revizuire.

3.4 Să asigure integrarea controalelor criptografice în etapa de proiectare a sistemelor și validarea periodică a acestora pentru a preveni expunerea datelor, compromiterea cheilor sau degradarea protocoalelor.

3.5 Să impună gestionarea ciclului de viață al tuturor cheilor criptografice, inclusiv generarea, stocarea, utilizarea, rotația, revocarea și distrugerea securizată a acestora.

3.6 Să respecte reglementările internaționale și regionale care impun criptarea și gestionarea securizată a datelor, inclusiv GDPR, DORA, NIS2 și COBIT 2019.

4. Roluri și responsabilități

4.1 Managerul securității informației / Directorul de securitate a informațiilor

4.1.1 Deține această politică și asigură alinierea acesteia cu SMSI și cu Controlul 8.24 din Anexa A a ISO/IEC 27001.

4.1.2 Aprobă utilizarea algoritmilor și controalelor criptografice și impune respectarea cerințelor acestei politici la nivelul întregii organizații.

4.2 Responsabilul operațiunilor criptografice / Arhitectul de securitate

4.2.1 Gestionează operațiunile curente și administrarea sistemelor criptografice.

4.2.2 Menține Lista metodelor criptografice aprobate (ACML) și Registrul de management al cheilor.

4.2.3 Efectuează revizuiri ale proiectării criptografice (CDR) și evaluează noile tehnologii criptografice.

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

9. Cerințe de revizuire și actualizare

9.1 Această politică trebuie revizuită anual de Managerul securității informației și de Responsabilul operațiunilor criptografice.

9.2 Declanșatorii revizuirii includ:

9.2.1 descoperirea unor vulnerabilități criptografice (de exemplu, downgrade de algoritmi, atacuri cuantice)

9.2.2 modificări de reglementare care impun standarde actualizate de criptare

9.2.3 constatări operaționale sau de audit care evidențiază deficiențe de control

9.2.4 modernizări ale instrumentelor criptografice sau schimbări de arhitectură

9.3 Actualizările trebuie supuse controlului versiunilor în Registrul de control al documentelor din SMSI și comunicate către:

9.3.1 toți administratorii cu roluri de acces criptografic

9.3.2 echipele de dezvoltare și responsabilii DevSecOps

9.3.3 furnizorii terți care au obligații contractuale privind criptarea

9.4 Echipa SMSI trebuie să se asigure că versiunile înlocuite sunt arhivate și nu mai sunt referențiate în procedurile operaționale.

10. Politici conexe și interdependențe

10.1 P1 - Politica de securitate a informației. Oferă baza de guvernanță pentru toate măsurile de securitate, inclusiv aplicarea controalelor criptografice, protecția activelor și comunicațiile securizate.

10.2 P4 - Politica de control al accesului. Asigură că accesul logic la materialele criptografice și la sistemele de management al criptării este limitat strict pe baza principiului privilegiului minim și a separării atribuțiilor.

10.3 P6 - Politica de management al riscurilor. Susține evaluarea riscurilor asociate controalelor criptografice și documentează strategia de tratare a riscului pentru excepții, învechirea algoritmilor sau scenarii de compromitere a cheilor.

10.4 P12 - Politica de management al activelor. Impune clasificarea datelor sensibile și a activelor hardware, care determină în mod direct cerințele criptografice și obligațiile privind custodia cheilor.

10.5 P13 - Politica de clasificare și etichetare a datelor. Definește nivelurile de clasificare (de exemplu, Confidențial, Reglementat) care declanșează cerințe specifice de criptare în tranzit și în repaus.

10.6 P14 - Politica de retenție și eliminare a datelor. Specifică procedurile pentru eliminarea securizată a mediilor de stocare criptate și a materialului criptografic al cheilor la sfârșitul ciclului de viață.

10.7 P30 - Politica de răspuns la incidente. Prezintă strategia organizației de răspuns pentru compromiterea cheilor, utilizarea abuzivă a certificatelor sau suspiciunile privind vulnerabilități algoritmice, inclusiv revocarea rapidă și raportarea încălcărilor de securitate.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 - Planificare și control operațional: impune controale tehnice de securitate, inclusiv măsuri criptografice, ca parte a măsurilor operaționale de protecție.

11.2 ISO/IEC 27002:2022

11.2.1 Controalele 8.24, 8.25, 8: oferă orientări de implementare privind obiectivele controalelor criptografice, selectarea algoritmilor, aplicarea protocoalelor și managementul ciclului de viață al certificatelor.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 - Stabilirea cheilor criptografice: asigură generarea și schimbul securizat al cheilor de criptare. P18 definește modul în care cheile simetrice și asimetrice trebuie generate și schimbate utilizând algoritmi și protocoale aprobate.

11.3.2 SC-13 - Protecție criptografică: impune utilizarea criptografiei pentru protejarea confidențialității și integrității informațiilor. P18 aplică criptarea în repaus și în tranzit pe baza clasificării datelor, cu standarde algoritmice aliniate la NIST FIPS 140-3.

11.3.3 SC-17 - Certificate ale infrastructurii cu chei publice (PKI): impune implementarea PKI pentru a susține autentificarea și semnăturile digitale. P18 descrie utilizarea PKI pentru securizarea comunicațiilor, a identităților sistemelor și a accesului administrativ.

11.3.4 SC-28, SC-28(1) - Protecția informațiilor în repaus și în tranzit: impune criptarea datelor atunci când sunt stocate sau transmise prin rețele care nu sunt de încredere. P18 specifică aplicarea TLS, a tunelurilor VPN, a criptării complete a discului și a metodelor de stocare securizată pentru date sensibile.

11.3.5 SC-12(3) - Generarea cheilor simetrice pentru stocare și distribuire securizate: se concentrează pe generarea și gestionarea securizată a cheilor simetrice. P18 impune utilizarea

unor generatori puternici de numere aleatoare, a politicilor de rotație a cheilor și a seifurilor securizate pentru chei în operațiunile criptografice.

11.4 GDPR UE (2016/679)

11.4.1 Articolul 32 - Securitatea prelucrării: recomandă în mod explicit criptarea ca măsură de reducere a riscului pentru datele cu caracter personal.

11.4.2 Considerentul 83: subliniază criptarea ca mecanism de control pentru prevenirea accesului neautorizat la date.

11.4.3 Articolele 33 și 34: criptarea poate excepta organizațiile de la obligațiile de notificare obligatorie a încălcărilor de securitate, dacă este eficace.

11.5 Directiva UE NIS2 (2022/2555)

11.5.1 Articolul 21(2)(d): impune măsuri tehnice și organizatorice, inclusiv protecții criptografice, pentru menținerea disponibilității și integrității serviciilor.

11.6 Regulamentul UE DORA (2022/2554)

11.6.1 Articolul 6(2)(d): instituțiile financiare trebuie să securizeze datele, inclusiv prin criptarea puternică a informațiilor critice.

11.6.2 Articolul 11(1)(c): impune controale de securitate pentru prelucrarea datelor de către furnizorii terți de servicii TIC.

11.7 COBIT 2019

11.7.1 DSS05.01 - Protejarea activelor informaționale: impune utilizarea criptării și a managementului cheilor pentru protejarea datelor împotriva accesului neautorizat.

11.7.2 DSS06.06 - Testare de securitate gestionată: recomandă validarea conformității criptografice ca parte a evaluărilor de vulnerabilitate.

11.7.3 MEA03 - Monitorizarea, evaluarea și analizarea conformității: impune asigurarea continuă a eficacității controalelor criptografice.