					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P18S					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	
NIST SP 800-53 Rev. 5	SC-12 până la SC-17	
Directiva UE NIS2	Articolele 21(2)(d), 21(2)(e)	
Regulamentul UE DORA	Articolele 6(2)(d), 9(2)(f)	
COBIT 2019	DSS05.01, APO13	
RGPD al UE	Articolele 32(1)(a), 34	

1. Scop

1.1 Prezenta politică stabilește cerințe obligatorii privind utilizarea criptării și a controalelor criptografice pentru protejarea confidențialității, integrității și autenticității datelor de afaceri și a datelor cu caracter personal.

1.2 Aceasta asigură utilizarea adecvată a mecanismelor criptografice la nivelul sistemelor, dispozitivelor și serviciilor cloud, într-un mediu specific întreprinderilor mici.

1.3 Prezenta politică sprijină în mod direct certificarea ISO/IEC 27001:2022 și ajută organizația să își îndeplinească obligațiile legale prevăzute de RGPD, Directiva UE NIS2 și Regulamentul UE DORA.

1.4 Controalele criptografice vizate includ criptarea datelor, managementul certificatelor, gestionarea securizată a cheilor și backupurile criptate.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică:

2.1.1 tuturor angajaților, contractorilor și terților care gestionează datele companiei;

2.1.2 tuturor sistemelor de afaceri, stațiilor terminale și platformelor cloud utilizate pentru stocarea, transmiterea sau accesarea informațiilor confidențiale;

2.1.3 tuturor înregistrărilor cu caracter personal, financiare, juridice sau sensibile clasificate conform politicii organizației privind clasificarea datelor;

2.1.4 oricărui control criptografic, inclusiv metodelor de criptare, cheilor, parolelor, certificatelor și modulelor de securitate.

2.2 Politica acoperă datele în repaus, datele în tranzit și datele în utilizare. De asemenea, reglementează criptarea utilizată pentru backupuri, poșta electronică, transferurile externe de date și site-urile web publice.

3. Obiective

3.1 Să asigure protecția continuă a datelor sensibile și a datelor reglementate prin măsuri criptografice adecvate.

3.2 Să definească responsabilitățile privind selecția mecanismelor de criptare, configurarea acestora și managementul cheilor.

3.3 Să prevină accesul neautorizat, alterarea sau divulgarea neautorizată a datelor prin aplicarea controalelor de transmitere și stocare securizate.

3.4 Să asigure conformitatea cu cerințele legale și de reglementare care impun criptarea datelor cu caracter personal și a datelor de afaceri.

3.5 Să mențină securitatea operațională și disponibilitatea prin gestionarea eficace a certificatelor și a cheilor criptografice.

4. Roluri și responsabilități

4.1 Director general (GM)

4.1.1 Aprobă prezenta politică și se asigură că cerințele criptografice sunt aplicate.

4.1.2 Revizuiește excepțiile, notificările privind incidentele de securitate și conformitatea furnizorilor cu clauzele privind criptarea.

4.1.3 Verifică faptul că serviciile externalizate sau serviciile cloud respectă standardele de criptare.

4.2 Furnizorul de servicii IT / Administratorul IT intern

4.2.1 Implementează și menține soluții de criptare (de exemplu, criptarea completă a discului, certificate SSL, VPN-uri).

4.2.2 Gestionează ciclul de viață al cheilor criptografice și mecanismele de stocare securizată.

4.2.3 Configurează și monitorizează criptarea pentru protecția backupurilor, site-urilor web și dispozitivelor.

[... 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 Revizuire anuală

9.1.1 Prezenta politică trebuie revizuită cel puțin o dată pe an de Directorul general, în coordonare cu furnizorul de servicii IT și Responsabilul cu protecția datelor.

9.2 Declanșatoare pentru revizuire intermediară

9.2.1 Revizuirile trebuie efectuate și în cazul în care:

9.2.1.1 standardele sau protocoalele criptografice se modifică (de exemplu, deprecierea unui algoritm);

9.2.1.2 sunt introduse sisteme noi sau servicii cloud;

9.2.1.3 o încălcare sau un incident implică o cheie sau un certificat compromis;

9.2.1.4 actualizările legale sau de reglementare afectează cerințele privind criptarea.

9.3 Controlul versiunilor și comunicare

9.3.1 Toate modificările politicii trebuie documentate într-un jurnal al versiunilor.

9.3.2 Personalul trebuie notificat cu privire la actualizări, iar versiunile anterioare trebuie arhivate.

9.3.3 Cea mai recentă versiune aprobată trebuie stocată în registrul central al politicilor.

10. Politici asociate și interdependențe

10.1 Prezenta politică trebuie aplicată împreună cu următoarele politici SME:

10.1.1 P12S – Politica de management al activelor: Asigură aplicarea criptării asupra activelor clasificate pe durata stocării, transferului și eliminării.

10.1.2 P14S – Politica de retenție și eliminare a datelor: Definește perioadele de retenție și impune stocarea criptată a datelor până la eliminarea securizată.

10.1.3 P17S – Politica de protecție a datelor și confidențialitate: Aliniază criptarea la principiile de protecție a datelor și la cerințele de reglementare prevăzute la articolul 32 din RGPD.

10.1.4 P22S – Politica de jurnalizare și monitorizare: Impune jurnalizarea utilizării cheilor, a eșecurilor de criptare și a expirării certificatelor în scop de audit.

10.1.5 P30S – Politica de răspuns la incidente: Detaliază procedurile de escaladare, limitare a impactului și notificare atunci când criptarea eșuează sau cheile sunt compromise.

11. Standarde și cadre de referință

11.1 ISO/IEC 27001

11.1.1 Clauza 8.1 – Impune implementarea controalelor operaționale, inclusiv a criptării, pentru gestionarea riscurilor de securitate.

11.2 ISO/IEC 27002

11.2.1 Controlul 8.24 – Descrie cerințele pentru aplicarea criptării în scopul asigurării confidențialității și integrității.

11.2.2 Controlul 8.25 – Prezintă cerințele privind managementul securizat al cheilor criptografice și al certificatelor.

11.3 NIST SP 800-53 Rev. 5

11.3.1 SC-12 – Stabilește cerințe privind stabilirea și validarea cheilor criptografice.

11.3.2 SC-13 – Definește standarde pentru generarea cheilor criptografice.

11.3.3 SC-17 – Acoperă infrastructura cu chei publice (PKI) și managementul ciclului de viață al certificatelor.

11.3.4 SC-28 – Impune criptarea datelor în repaus.

11.3.5 SC-12 până la SC-17 (familie) – Asigură implementarea corespunzătoare a protecțiilor criptografice la nivelul sistemelor.

11.4 RGPD

11.4.1 Articolul 32(1)(a) – Impune organizațiilor implementarea de măsuri tehnice, precum criptarea, pentru asigurarea confidențialității datelor.

11.4.2 Articolul 34 – Prevede că utilizarea criptării poate excepta organizațiile de la notificarea încălcărilor, dacă datele erau neinteligibile pentru persoanele neautorizate.

11.5 Directiva UE NIS2

11.5.1 Articolul 21(2)(d) – Impune criptare eficace pentru securizarea sistemelor și comunicațiilor.

11.5.2 Articolul 21(2)(e) – Evidențiază protecția datelor și atenuarea amenințărilor cibernetice prin criptare.

11.6 Regulamentul UE DORA

11.6.1 Articolul 6(2)(d) – Impune menținerea unor canale de comunicații securizate și utilizarea criptării în sistemele TIC.

11.6.2 Articolul 9(2)(f) – Obligă entitățile financiare să utilizeze criptare puternică pentru protejarea comunicațiilor digitale și a schimburilor de date.

11.7 COBIT 2019

11.7.1 DSS05.01 – Impune protejarea informațiilor sensibile prin criptare și protocoale criptografice.

11.7.2 APO13.02 – Impune implementarea eficace a controalelor de securitate, inclusiv a măsurilor criptografice de protecție, ca parte a planificării securității informației.