					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P31					Titlul documentului: **Politica privind colectarea probelor și activitățile criminalistice**							
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 5.25–5.27, 8.27	
ISO/IEC 27035:2016	Părțile 1 și 3	
NIST SP 800-53 Rev. 5	IR-1 până la IR-9, AU-6, PL-2	
NIST SP 800-101 Rev. 1	Criminalistică pentru dispozitive mobile și medii de stocare	Criminalistică pentru dispozitive mobile și medii de stocare
NIST SP 800-86	Integrarea tehnicilor criminalistice	Integrarea tehnicilor criminalistice în răspunsul la incidente
GDPR	Articolele 5, 33–34	
Directiva NIS2	Articolul 23 alin. (1)–(4)	
Regulamentul DORA	Articolul 17 alin. (1)–(3)	
COBIT 2019	DSS01.07, DSS05.04	

1. Scop

1.1 Prezenta politică stabilește un cadru structurat și solid din punct de vedere juridic pentru identificarea, colectarea, conservarea, analiza și eliminarea probelor digitale în contextul incidentelor de securitate confirmate sau suspectate.

1.2 Aceasta asigură că procesele de pregătire criminalistică și de gestionare a probelor:

1.2.1 mențin integritatea probatorie și lanțul de custodie;

1.2.2 sprijină investigațiile interne, procedurile judiciare sau raportarea către autoritățile de reglementare;

1.2.3 sunt aliniate la standardele criminalistice acceptate la nivel internațional și la criteriile de admisibilitate legală.

1.3 Politica sprijină angajamentul organizației privind răspunsul proactiv la incidente, conformitatea juridică și transparența guvernanței, reducând totodată la minimum impactul asupra activităților operaționale ale organizației.

2. Domeniu de aplicare

2.1 Prezenta politică se aplică următoarelor categorii:

2.1.1 tuturor angajaților, contractorilor, furnizorilor și prestatorilor de servicii implicați în administrarea sistemelor, gestionarea incidentelor sau activități de investigație;

2.1.2 tuturor stațiilor de lucru, serverelor, aplicațiilor, rețelelor și platformelor cloud aflate sub controlul organizației sau în responsabilitatea sa contractuală;

2.1.3 oricărui incident sau eveniment care impune gestionarea probelor, inclusiv:

2.1.3.1 amenințări interne, încălcări ale securității datelor sau investigații privind frauda;

2.1.3.2 utilizarea abuzivă a sistemelor sau a acreditărilor;

2.1.3.3 incidente aferente sistemelor de tehnologie operațională (OT) sau de control industrial;

2.1.3.4 încălcări ale regulilor de acces fizic care implică active digitale.

2.2 Politica reglementează, de asemenea, orice interacțiune cu servicii criminalistice furnizate de terți sau cu organele de aplicare a legii în cadrul escaladărilor juridice ori al procedurilor de reglementare.

3. Obiective

3.1 Să permită obținerea rapidă, securizată și conformă cu politica a probelor în cadrul evenimentelor de securitate sau al investigațiilor.

3.2 Să păstreze integritatea, autenticitatea și admisibilitatea probelor digitale colectate prin control strict al accesului, jurnalizare și proceduri de verificare.

3.3 Să asigure corelarea tuturor activităților criminalistice cu obligațiile juridice și de reglementare, inclusiv cele privind protecția datelor, dreptul muncii și restricțiile privind transferurile internaționale.

3.4 Să sprijine analiza post-incident, determinarea cauzei principale și îmbunătățirea controalelor prin rezultate criminalistice de înaltă calitate.

3.5 Să integreze pregătirea criminalistică în cadrul general al Sistemului de management al securității informației (SMSI), pentru a sprijini auditurile, notificarea încălcărilor și procesul decizional al conducerii executive.

4. Roluri și responsabilități

4.1 Directorul de securitate a informațiilor (CISO)

4.1.1 Deține această politică și se asigură că toate operațiunile criminalistice sunt susținute juridic, verificabile și bazate pe risc.

4.1.2 Autorizează escaladarea către entități juridice externe și furnizori de servicii criminalistice.

4.2 Analiști criminaliști / responsabili cu gestionarea incidentelor

4.2.1 Coordonează obținerea, conservarea și analiza tehnică a probelor.

4.2.2 Se asigură că lanțul de custodie este înregistrat și menținut corespunzător.

4.2.3 Documentează toate acțiunile, constatările și configurațiile instrumentelor utilizate pe durata investigațiilor.

[... 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 Prezenta politică trebuie revizuită cel puțin anual și actualizată, după caz, pentru a reflecta:

9.1.1 modificările legislative, de reglementare sau de jurisprudență care afectează procedurile criminalistice sau gestionarea datelor;

9.1.2 actualizările standardelor sau seturilor de instrumente criminalistice recunoscute în industrie;

9.1.3 lecțiile învățate din revizuiri post-incident, litigii sau constatări de audit;

9.1.4 schimbările tehnologice privind platformele, dispozitivele sau sistemele aflate în investigație.

9.2 Procesul de revizuire este deținut de CISO și trebuie să includă consultarea următoarelor funcții:

9.2.1 juridic și conformitate;

9.2.2 Responsabilul cu protecția datelor (DPO);

9.2.3 echipele de operațiuni de securitate și criminalistică;

9.2.4 audit intern.

9.3 Toate revizuirile trebuie:

9.3.1 să fie supuse controlului versiunilor și stocate în depozitul de politici;

9.3.2 să fie comunicate părților interesate afectate, inclusiv echipelor criminalistice și de răspuns;

9.3.3 să fie însoțite de actualizări ale procedurilor operaționale relevante și ale materialelor de instruire.

9.4 Revizuirile intermediare trebuie declanșate după orice incident critic care implică gestionarea necorespunzătoare a probelor, compromiterea lanțului de custodie sau probleme de admisibilitate legală.

10. Politici conexe și interdependențe

10.1 Prezenta politică este aliniată și susținută de următoarele politici ale organizației:

10.1.1 P1 – Politica de securitate a informației: stabilește mandatul de bază pentru investigații, controlul probelor și conformitatea cu legislația aplicabilă.

10.1.2 P5 – Politica de management al schimbărilor: asigură că sistemele aflate în investigație nu sunt modificate pe durata proceselor criminalistice active.

10.1.3 P14 – Politica de păstrare și eliminare a datelor: reglementează eliminarea securizată și termenele de păstrare pentru probe și date aferente cazurilor.

10.1.4 P18 – Politica privind controalele criptografice: stabilește cerințele de criptare pentru stocarea și transferul datelor sensibile sau cu valoare probatorie.

10.1.5 P22 – Politica de jurnalizare și monitorizare: asigură disponibilitatea jurnalelor de evenimente și a telemetriei pentru colectarea probelor și corelarea criminalistică.

10.1.6 P30 – Politica de răspuns la incidente: definește triajul incidentelor și traseele de escaladare în cadrul cărora sunt declanșate procedurile criminalistice.

10.1.7 P33 – Politica de audit și monitorizare a conformității: validează respectarea protocoalelor criminalistice și a cerințelor privind lanțul de custodie prin audituri periodice.

11. Standarde și cadre de referință

11.1 Prezenta politică este aliniată la standardele internaționale privind activitățile criminalistice și gestionarea incidentelor, asigurând integritatea probelor, susținerea juridică și conformitatea în contexte multijurisdicționale.

11.2 ISO/IEC 27001

11.2.1 Clauza 8.1 – Sprijină planificarea și controlul operațional pentru pregătirea criminalistică și procedurile privind probele.

11.3 ISO/IEC 27002

11.3.1 Anexa A, controlul 5.25 – Responsabilități privind managementul incidentelor: impune roluri definite pentru gestionarea incidentelor de securitate a informației și a investigațiilor.

11.3.2 Anexa A, controlul 5.26 – Raportarea evenimentelor de securitate a informației: sprijină colectarea artefactelor asociate evenimentelor ca probe.

11.3.3 Anexa A, controlul 5.27 – Răspuns la incidente de securitate a informației: impune remediere și investigație structurate, bazate pe probe.

11.3.4 Anexa A, controlul 8.27 – Dezvoltare securizată și activități criminalistice (unde este aplicabil): abordează protejarea sistemelor și a instrumentelor în timpul investigațiilor.

11.4 ISO/IEC 27035:2016 (Părțile 1 și 3)

11.4.1 Prezintă principiile detectării incidentelor, răspunsului și pregătirii criminalistice, inclusiv planificarea, lanțul de custodie și managementul probelor aferente incidentelor.

11.5 NIST SP 800-53 Rev. 5

11.5.1 IR-1 până la IR-9, AU-6, PL-2: definesc cerințe structurate pentru planificarea, detectarea, analiza, limitarea impactului și răspunsul la incidente de securitate. Sprijină colectarea și caracterul verificabil al probelor (AU-6) și asigură alinierea cu planurile de securitate și confidențialitate ale sistemelor (PL-2) în cadrul investigațiilor criminalistice.

11.6 NIST SP 800-86

11.6.1 Oferă orientări privind integrarea proceselor criminalistice în ciclul de viață mai larg al răspunsului la incidente și privind asigurarea pregătirii criminalistice.

11.7 NIST SP 800-101 Rev. 1

11.7.1 Se concentrează pe bune practici pentru obținerea, conservarea și analiza probelor din medii digitale și dispozitive mobile într-un mod solid din punct de vedere juridic.

11.8 GDPR (UE) 2016/679

11.8.1 Articolul 5 – Principii referitoare la prelucrarea datelor cu caracter personal: se aplică probelor care conțin date cu caracter personal sau date sensibile, asigurând reducerea la minimum a datelor și limitarea scopului.

11.8.2 Articolele 33–34 – notificarea încălcărilor: datele criminalistice sprijină conformitatea cu obligațiile de notificare a încălcărilor și cu procedurile de divulgare legală.

11.9 Directiva NIS2 a UE (2022/2555)

11.9.1 Articolul 23 – Obligații de raportare: documentația criminalistică și constatările sprijină transmiterea la timp și cu acuratețe a rapoartelor de incident către autoritățile competente.

11.10 Regulamentul DORA al UE (2022/2554)

11.10.1 Articolul 17 – Raportarea incidentelor TIC: impune înregistrări detaliate privind cauza principală și probele aferente incidentelor majore legate de TIC, în special în sectorul financiar.

11.11 COBIT 2019

11.11.1 DSS01.07 – Gestionarea incidentelor de securitate: impune documentarea incidentelor și rigoare în investigație.

11.11.2 DSS05.04 – Gestionarea investigațiilor de securitate: pune accent pe conservarea probelor digitale și pe sprijinul pentru acțiuni disciplinare și juridice.