					Introduceți aici denumirea entității juridice înregistrate							
Numărul documentului: P31S					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	Clauzele 6.1, 6.3, 8	Planificare bazată pe risc, acțiuni de îmbunătățire și controale operaționale pentru integritatea probelor
ISO/IEC 27002:2022	Controalele 5.24–5.27	Ghidează gestionarea securizată, revizuirea post-incident și îmbunătățirile bazate pe probe
ISO/IEC 27035-3:2016	Clauzele 6.3, 6.4, 7	Asigură planificarea adecvată, colectarea legală și gestionarea securizată a probelor digitale, cu documentarea lanțului de custodie
NIST SP 800-53 Rev.5	IR-07, IR-08, AU-09, AU-12, PE-18	Pregătire criminalistică, protecția jurnalelor de audit, integrare eficace în răspunsul la incidente
GDPR al UE	Articolele 33, 34	Documentare și trasabilitate pentru încălcările securității datelor cu caracter personal
Directiva NIS2 a UE	Articolul 23	Raportare trasabilă a incidentelor și gestionare securizată a probelor
Regulamentul DORA al UE	Articolul 17(1), 17(2)	Asigură colectarea, stocarea și păstrarea probelor pentru incidente legate de TIC, rigurozitate criminalistică și răspuns la solicitările autorităților de reglementare
COBIT 2019	DSS05.06, DSS05.07	Jurnalizare fiabilă și gestionare structurată a probelor pentru investigații securizate și verificabile

1. Scop

1.1. Prezenta politică definește modul în care organizația gestionează probele digitale aferente incidentelor de securitate, încălcărilor securității datelor sau investigațiilor interne. Aceasta asigură colectarea, stocarea și păstrarea probelor într-un mod defensabil din punct de vedere juridic și pregătit pentru audit, sprijinind atât procesul decizional intern, cât și eventualele demersuri externe.

1.2. Politica permite organizațiilor mici să protejeze integritatea jurnalelor, fișierelor și imaginilor de sistem, demonstrând totodată diligența necesară în conformitate cu ISO/IEC 27001, GDPR și standardele conexe.

1.3. Aceasta susține pregătirea criminalistică fără a necesita resurse tehnice avansate sau o echipă IT dedicată, prin definirea clară a responsabilităților, proceselor și cerințelor de păstrare.

2. Domeniu de aplicare

2.1. Prezenta politică se aplică următoarelor:

2.1.1. Tuturor angajaților, furnizorilor de servicii IT și consultanților externi implicați în răspunsul la incidente, investigații sau analiza încălcărilor de securitate

2.1.2. Tuturor sistemelor companiei, inclusiv laptopurilor, dispozitivelor mobile, serverelor, conturilor de e-mail, platformelor SaaS și spațiilor de stocare în cloud (de exemplu, Microsoft 365, Google Workspace)

2.1.3. Oricărui eveniment care necesită probe pentru acțiuni disciplinare interne, apărare juridică, cereri de despăgubire în baza asigurării sau interacțiuni cu autoritățile de reglementare

2.2. Aceasta include atât evenimente reale, cât și suspectate, care implică:

2.2.1. Scurgeri de date

2.2.2. Amenințări interne sau utilizare abuzivă

2.2.3. Încălcări ale securității (de exemplu, malware, acces neautorizat)

2.2.4. Reclamații ale clienților care necesită validare digitală

2.2.5. Solicitări din partea autorităților de reglementare sau a organelor de aplicare a legii

3. Obiective

3.1. Să asigure că toate probele sunt colectate și gestionate într-un mod care le menține integritatea, autenticitatea și lanțul de custodie.

3.2. Să prevină modificarea accidentală, ștergerea sau gestionarea necorespunzătoare a jurnalelor, fișierelor ori imaginilor de sistem care pot fi necesare pentru investigații.

3.3. Să asigure o abordare consecventă și verificabilă pentru gestionarea probelor, care să îndeplinească cerințele legale și de reglementare (de exemplu, notificarea încălcărilor în temeiul GDPR, trasabilitatea în temeiul NIS2).

3.4. Să definească roluri și responsabilități clare pentru a asigura captarea rapidă, securizată și conformă cu cerințele legale a probelor în timpul incidentelor de securitate.

3.5. Să susțină pregătirea criminalistică la nivelul IMM-urilor, reducând în același timp complexitatea și evitând perturbarea activităților curente ale organizației.

4. Roluri și responsabilități

4.1. Director general

4.1.1. Aprobă toate investigațiile formale care necesită colectarea de probe.

4.1.2. Revizuiește și aprobă rapoartele de incident care implică posibile acțiuni juridice sau disciplinare.

4.1.3. Decide dacă trebuie implicați consultanți juridici externi sau notificate autorități de reglementare.

4.1.4. Se asigură că politica este revizuită și actualizată periodic.

4.2. Furnizor de servicii IT / Administrator de sistem

4.2.1. Colectează și păstrează probele digitale în conformitate cu proceduri securizate.

4.2.2. Documentează marcajele temporale, detaliile sistemului și etapele de manipulare.

4.2.3. Securizează toate materialele colectate într-o locație protejată.

4.2.4. Oferă sprijin pentru analiza criminalistică, dacă este necesar.

[... 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. Revizuirea anuală a politicii

9.1.1. Această politică trebuie revizuită cel puțin o dată la 12 luni de către Directorul general, pentru a confirma:

9.1.1.1. Conformitatea cu controalele din Anexa A la ISO/IEC 27001

9.1.1.2. Relevanța continuă pentru platformele digitale și serviciile IT actuale

9.1.1.3. Adecvarea procedurilor de jurnalizare, păstrare a probelor și pregătire criminalistică

9.2. Evenimente declanșatoare pentru revizuirea politicii

9.2.1. Politica trebuie, de asemenea, revizuită și actualizată după:

9.2.1.1. Orice incident major care necesită colectarea de probe

9.2.1.2. Un audit nefavorabil sau o solicitare din partea unei autorități de reglementare în care integritatea probelor a fost pusă sub semnul întrebării

9.2.1.3. Adoptarea de noi instrumente sau proceduri pentru răspunsul la incidente ori monitorizarea sistemelor

9.2.1.4. Modificări legislative (de exemplu, actualizări ale orientărilor GDPR sau NIS2)

9.3. Aprobarea și distribuirea modificărilor

9.3.1. Toate modificările trebuie revizuite și aprobate de Directorul general

9.3.2. Versiunea actualizată trebuie distribuită către:

9.3.2.1. Furnizorii de servicii IT și consultanții implicați în investigații

9.3.2.2. Orice membru al personalului cu responsabilități de administrare a sistemelor

9.3.3. O copie actualizată trebuie păstrată în arhiva de politici a companiei și pusă la dispoziția auditorilor, la cerere

10. Politici conexe și interdependențe

10.1. Prezenta politică este interdependentă cu următoarele politici pentru IMM-uri:

10.1.1. P2S – Politica privind rolurile și responsabilitățile de guvernanță: stabilește autoritatea asupra investigațiilor incidentelor, deciziilor privind probele și escaladării juridice.

10.1.2. P4S – Politica de control al accesului: asigură că numai personalul autorizat poate accesa sistemele sensibile și jurnalele în timpul investigațiilor.

10.1.3. P22S – Politica de jurnalizare și monitorizare: furnizează datele brute utilizate ca probe criminalistice și stabilește cerințele privind păstrarea, controlul accesului și jurnalizarea.

10.1.4. P30S – Politica de răspuns la incidente: declanșează necesitatea colectării de probe și definește fluxul operațional care conduce la păstrarea în condiții criminalistice.

10.1.5. P17S – Politica de protecție a datelor și confidențialitate: asigură că orice date cu caracter personal colectate ca probe sunt gestionate legal în temeiul GDPR și al reglementărilor conexe.

10.2. Aceste politici funcționează împreună pentru a susține defensabilitatea juridică, integritatea investigațiilor și pregătirea completă pentru audit în conformitate cu ISO/IEC 27001:2022.

11. Standarde și cadre de referință

11.1. ISO/IEC 27001

11.1.1. Clauza 6.1 – Planificarea bazată pe risc include pregătirea pentru răspuns și procedurile privind probele.

11.1.2. Clauza 6.3 – Susține acțiunile de îmbunătățire bazate pe probe rezultate din incidente.

11.1.3. Clauza 8.1 – Impune controale operaționale pentru integritatea probelor.

11.2. ISO/IEC 27002

11.2.1. Controalele 5.24–5.27 – Ghidează gestionarea securizată, revizuirea post-incident și îmbunătățirile bazate pe probe.

11.3. ISO/IEC 27035-3

11.3.1. Clauzele 6.3, 6.4 și 7.3 asigură planificarea adecvată, colectarea legală și gestionarea securizată a probelor digitale în timpul răspunsului la incidente, inclusiv păstrarea și documentarea lanțului de custodie.

11.4. NIST SP 800-53 Rev. 5

11.4.1. IR-07, IR-08, AU-09 și AU-12 asigură pregătirea criminalistică, protecția jurnalelor de audit și integrarea eficace a colectării probelor în ciclul de viață al răspunsului la incidente

11.5. NIST SP 800-86

11.5.1. Definește cele mai bune practici pentru achiziția, analiza și protejarea probelor digitale în timpul răspunsului la incidente.

11.6. GDPR al UE

11.6.1. Articolele 33–34 – Impun documentarea și trasabilitatea incidentelor și a probelor atunci când sunt raportate încălcări ale securității datelor cu caracter personal.

11.7. Directiva NIS2 a UE (2022/2555)

11.7.1. Articolul 23 – Impune raportarea trasabilă a incidentelor și gestionarea securizată a probelor pentru entitățile esențiale și importante.

11.8. Regulamentul DORA al UE

11.8.1. Articolul 17(1) – Asigură că probele legate de incidente TIC sunt colectate și stocate într-un mod care susține investigațiile criminalistice.

11.8.2. Articolul 17(2) – Impune ca entitățile financiare să păstreze toate datele și jurnalele relevante asociate evenimentelor de securitate, în concordanță cu cerințele de rigurozitate criminalistică și cu solicitările autorităților de reglementare.

11.9. COBIT 2019

11.9.1. DSS05.06 – Monitorizarea, detectarea și raportarea incidentelor: pune accent pe jurnalizarea fiabilă pentru susținerea investigațiilor.

11.9.2. DSS05.07 – Investigarea incidentelor și adoptarea măsurilor necesare: impune gestionarea structurată a probelor pentru a permite investigații securizate și verificabile.