

Digital Civic Kit

Cele șase documente-model, într-un singur fișier · 2026-09-16

Ediție de comoditate. Fiecare document se adoptă separat și funcționează singur. Acest fișier le adună doar pentru tipărire și arhivare. Dacă adoptați un singur document, luați-l pe cel din folderul lui, cu anexele lui.

Cuprins

#	Document	Se livrează
1	Politica privind protecția datelor cu caracter personal și gestionarea informațiilor	documentul 3 din kit
2	Politica de utilizare a instrumentelor digitale și management al conturilor	documentul 1 din kit
3	Politica de securitate digitală și răspuns la incidente	documentul 2 din kit
4	Procedură de management digital al proiectelor, documentelor și datelor	documentul 5 din kit
5	Politica privind utilizarea responsabilă a inteligenței artificiale	documentul 4 din kit
6	Ghid practic: serviciile publice digitale și relația digitală cu statul și cu finanțatorii	documentul 6 din kit

Politica privind protecția datelor cu caracter personal și gestionarea informațiilor

Documentul 3 din Digital Civic Kit · primul livrat · versiunea 1.0

Acesta este un document-model. Nu produce efecte în organizația dumneavoastră până nu îl adaptați și nu îl aprobați intern. Câmpurile marcate **[ASTFEL]** trebuie completate.

Fișa de adoptare

Câmp	De completat
Organizația	[NUMELE ORGANIZAȚIEI]
Documentul	Politica privind protecția datelor cu caracter personal și gestionarea informațiilor
Versiunea	1.0
Aprobat de	[ORGANUL CARE APROBĂ]
Data aprobării	[DATA]
Responsabil	[FUNCȚIA SAU PERSOANA]
Următoarea revizuire	[DATA]
Înlocuiește	[DOCUMENT ANTERIOR] sau „nimic”

0. Cum folosiți acest document

Citiți secțiunile 1 și 2, ca să știți ce acoperă. Completați fișa de adoptare. Parcurgeți regulile din secțiunea 6 și aplicați-le pe cele marcate N1. Aprobați documentul în organul care ia deciziile la dumneavoastră. Reveniți la el la data pe care ați scris-o în fișă.

Fiecare regulă poartă un nivel:

Nivel	Cui i se aplică
N1	Orice organizație, indiferent de mărime. Nu costă bani și nu cere pe cineva tehnic.
N2	Organizații de la 5 oameni în sus, sau care gestionează date ale beneficiarilor.
N3	Proiecte mari, date sensibile, expunere publică ridicată.

Dacă sunteți la început, aplicați N1 în întregime înainte să vă uitați la N2. Un document aplicat pe jumătate corect e mai bun decât unul citit în întregime și neaplicat.

1. Scop și rezultat așteptat

Organizația lucrează cu date despre oameni reali: beneficiari, participanți la instruiți, voluntari, donatori, angajați. Din 23 august 2026, felul în care aceste date sunt tratate e reglementat de o lege nouă, care se aplică deja. Documentul stabilește ce date colectează organizația, pe ce teme, cine are acces la ele, cât timp se păstrează și ce se face atunci când ceva merge prost.

Motivul nu e doar legal. O listă de beneficiari ajunsă unde nu trebuie e o problemă pentru oamenii din ea înainte să fie o problemă pentru organizație, iar într-un domeniu construit pe încredere aceasta e paguba care se repară cel mai greu.

Rezultatul așteptat: puteți răspunde, în cinci minute și fără să întrebați pe nimeni, la trei întrebări: ce date despre oameni aveți, unde stau, și cine are acces la ele.

2. Domeniu de aplicare

Se aplică tuturor persoanelor care prelucrează date în numele organizației: angajați, voluntari, membri ai organelor de conducere, stagiați și contractori. Se aplică indiferent de echipamentul folosit, inclusiv pe dispozitive personale, și indiferent de forma datelor, inclusiv pe hârtie.

Nu acoperă:

- măsurile tehnice de securitate și reacția la incidente cibernetice, care sunt tratate în documentul 2 din kit;
- organizarea documentelor de proiect și arhivarea lor, tratate în documentul 5;
- datele despre organizații ca entități juridice, care nu sunt date cu caracter personal; datele de contact ale unei persoane din acea organizație însă sunt.

3. Definiții

Date cu caracter personal. Orice informație care duce la o persoană identificabilă: nume, telefon, email, adresă, fotografie, IDNP, dar și un cod de participant pe care îl puteți corela cu un nume.

Persoană vizată. Omul despre care sunt datele.

Prelucrare. Orice faceți cu datele: colectare, stocare, consultare, transmitere, publicare, ștergere. Simpla păstrare a unei liste este prelucrare.

Operator. Cel care decide de ce și cum se prelucrează datele. Organizația dumneavoastră este operator pentru datele beneficiarilor săi.

Persoană împuternicită de operator. Cel care prelucrează date în numele dumneavoastră, după instrucțiunile dumneavoastră: un contabil extern, o firmă care găzduiește site-ul, un furnizor de servicii de email.

Temei legal. Motivul, dintre cele prevăzute de lege, pentru care aveți dreptul să prelucrați datele. Fără temei, prelucrarea e nelegală, oricât de bune ar fi intențiile.

Categorii speciale de date. Date despre sănătate, origine etnică, opinii politice, convingeri religioase, apartenență sindicală, viață sexuală, date biometrice și genetice. Regimul lor e mai strict.

Încălcarea securității datelor. Situația în care datele ajung la cine nu trebuie, se pierd, se distrug sau se modifică fără drept. Un laptop furat și un email trimis greșit sunt amândouă încălcări.

Consimțământ. Acordul liber, specific, informat și lipsit de ambiguitate al persoanei. Tăcerea nu e consimțământ, iar o căsuță bifată din start nu e consimțământ.

CNPDCP. Centrul Național pentru Protecția Datelor cu Caracter Personal, autoritatea de supraveghere din Republica Moldova (datepersonale.md).

4. Cadrul de referință

Legislația Republicii Moldova

- **Legea nr. 195 din 25 iulie 2024 privind protecția datelor cu caracter personal**, publicată în Monitorul Oficial al Republicii Moldova nr. 367-369 din 23 august 2024, art. 574. În vigoare din **23 august 2026**. Transpune integral Regulamentul (UE) 2016/679. Abrogă Legea nr. 133/2011.
- **Legea nr. 86/2020 cu privire la organizațiile necomerciale**, pentru obligațiile de raportare care presupun păstrarea unor documente.

Repere europene

- **Regulamentul (UE) 2016/679** privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal, cunoscut ca GDPR. Sursa transpunerii.
- **Convenția 108** a Consiliului Europei privind protecția persoanelor referitor la prelucrarea automatizată a datelor cu caracter personal, la care Republica Moldova este parte.
- **CNIL** (Commission nationale de l'informatique et des libertés, autoritatea franceză de protecție a datelor), pentru modelul de evidență a activităților de prelucrare, disponibil public și gratuit.

Ce prevede legea, pe scurt și cu articolele

Articolul	Ce cere
art. 5	Principiile: legalitate, scop determinat, date minime, exactitate, păstrare limitată, integritate și confidențialitate, responsabilitate
art. 6	Fiecare prelucrare are un temei legal
art. 7	Condițiile consimțământului
art. 8	Consimțământul copilului: pragul în Republica Moldova este 14 ani
art. 9	Categoriile speciale de date
art. 12-14	Informarea persoanei vizate
art. 15-22	Drepturile persoanei vizate
art. 30	Evidențele activităților de prelucrare
art. 32	Securitatea prelucrării
art. 33	Notificarea CNPDCP în cel mult 72 de ore de la încălcare
art. 34	Comunicarea încălcării către persoana vizată
art. 35	Evaluarea impactului, când riscul e ridicat
art. 37	Desemnarea responsabilului cu protecția datelor
art. 86-88	Amenzile
art. 90	Regimul tranzitoriu al amenzilor

Două lucruri de reținut din tabel. Amenzile sunt reduse temporar prin art. 90: se încasează 10% din cuantum în primul an de aplicare, 40% în al doilea, integral din al treilea. Reducerea privește doar amenda; obligațiile se aplică integral de la 23 august 2026.

Și responsabilul cu protecția datelor de la art. 37 **nu este obligatoriu pentru majoritatea organizațiilor mici**. Legea îl cere pentru autorități publice, pentru monitorizarea sistematică pe scară largă a persoanelor, și pentru prelucrarea pe scară largă a categoriilor speciale de date. Un OSC obișnuit nu se încadrează. Puteți desemna pe cineva responsabil intern, ceea ce e util, fără ca acesta să fie responsabilul în sensul legii.

5. Roluri și responsabilități

Rolul	Ce ține	Cine e la dumneavoastră
Responsabil de date	Ține evidența din Anexa 1, răspunde la cererile persoanelor, notifică incidentele	[NUME]
Conducerea	Aprobă documentul, decide în caz de incident, aprobă excepțiile	[NUME]
Coordonator de proiect	Aplică regulile la datele colectate în proiectul lui	[NUME]
Fiecare membru al echipei	Respectă regulile, semnalează imediat ce pare o scurgere	toți

Într-o organizație de trei oameni, rolurile de mai sus se comasează. Scrieți în dreptul fiecăruia numele persoanei care îl ține, chiar dacă e aceeași persoană de patru ori.

6. Reguli și proceduri

Ce date aveți

1. **N1** Completați evidența activităților de prelucrare din Anexa 1, cu toate activitățile prin care organizația atinge date despre oameni. Evidența e cerută de art. 30 și e, în practică, singurul mod de a răspunde la o întrebare despre datele voastre fără să improvizați.
2. **N1** Nu colectați date de care nu aveți nevoie. Înainte să adăugați o rubrică într-un formular, întrebați ce faceți concret cu răspunsul. Dacă nu aveți răspuns, scoateți rubrica.
3. **N2** Actualizați evidența la fiecare activitate nouă, nu o dată pe an.

Pe ce temei prelucrați

4. **N1** Fiecare activitate din evidență are un temei legal dintre cele de la art. 6, scris în dreptul ei: consimțământ, contract, obligație legală, interes vital, interes public sau interes legitim.
5. **N1** Consimțământul nu este temeiul implicit. Pentru un contract de voluntariat temeiul e contractul; pentru raportarea către Serviciul Fiscal de Stat e obligația legală. Alegerea greșită a temeiului vă obligă la lucruri care nu vi se aplică.
6. **N2** Dacă temeiul e consimțământul, păstrați dovada: cine, când și pentru ce a consimțit.
7. **N1** Pentru copii sub 14 ani, consimțământul îl dă sau îl autorizează reprezentantul legal. Pragul din Republica Moldova este 14 ani, mai jos decât cel implicit din regulamentul european.
8. **N3** Categoriile speciale de date, între care starea de sănătate și originea etnică, se prelucrează doar în cazurile limitate de la art. 9. Dacă un proiect vi le cere, tratați-le ca pe o decizie separată, nu ca pe o rubrică în plus.

Ce spuneți oamenilor

9. **N1** Spuneți persoanei, în momentul în care îi luați datele, cine sunteți, ce date luați, de ce, cât le păstrați și ce drepturi are. Modelul e în Anexa 2. Un paragraf clar e suficient; nu aveți nevoie de text juridic lung.
10. **N1** Orice formular online al organizației poartă nota de informare, inclusiv un formular Google făcut în cinci minute pentru o instruire.

Cine are acces

11. **N1** Accesul la date se dă după sarcină, nu după funcție. Cine nu are nevoie de lista de beneficiari pentru munca lui nu o primește.
12. **N1** Datele beneficiarilor nu circulă pe conturi personale de email și nu se lasă în grupuri de mesagerie. Un fișier trimis pe WhatsApp rămâne în telefoanele tuturor din grup și nu mai poate fi retras.
13. **N2** Contractorii și furnizorii care ating datele voastre primesc instrucțiuni scrise și o clauză de confidențialitate în contract. Un contabil extern e persoană împuternicită de operator, nu un terț oarecare.

Cât păstrați

14. **N1** Fiecare categorie de date din evidență are un termen de păstrare scris. „Cât e nevoie” nu e termen.
15. **N2** La expirarea termenului, ștergeți datele sau anonimiizați-le. Ștergerea include copiile din arhive, nu doar fișierul principal.
16. **N2** Termenele impuse de finanțator sau de legislația contabilă au prioritate față de termenul pe care l-ați ales dumneavoastră. Scrieți în evidență care e sursa termenului.

Fotografii și înregistrări

17. **N1** Fotografiile și înregistrările de la evenimente au nevoie de acord separat, dat înainte, nu presupus din prezența la eveniment. Modelul e în Anexa 4.
18. **N1** Fotografiile cu copii nu se publică fără acordul reprezentantului legal. Un acord dat pentru raportul către finanțator nu acoperă publicarea pe pagina de Facebook.
19. **N2** Păstrați acordurile acolo unde le găsiți repede, nu în dosarul evenimentului.

Când ceva merge prost

20. **N1** Orice suspiciune că datele au ajuns unde nu trebuie se anunță imediat responsabilului de date, în aceeași zi. Nu așteptați confirmarea că e o problemă reală.
21. **N1** Dacă încălcarea prezintă un risc pentru persoane, se notifică CNPDCP în cel mult 72 de ore de la momentul în care ați aflat, conform art. 33. Termenul curge din momentul aflării, nu din momentul în care lămuriiți ce s-a întâmplat, deci notificarea se face și cu informații incomplete, urmând să fie completată.
22. **N1** Dacă riscul pentru persoane e ridicat, persoanele afectate se anunță și ele, în limbaj simplu, conform art. 34.
23. **N2** Toate incidentele se consemnează, inclusiv cele care nu au fost notificate, cu motivul pentru care nu au fost.

Drepturile persoanelor

24. **N1** Orice persoană vă poate cere să îi spuneți ce date aveți despre ea, să le corectați, să le ștergeți sau să vă opriți din a le folosi. Răspundeți în cel mult o lună.
25. **N1** Cererea nu are formă obligatorie. Un mesaj pe pagina de Facebook a organizației este o cerere validă și termenul curge de la el.
26. **N2** Verificați identitatea celui care cere, înainte să trimiteți date. Cea mai simplă scurgere e cea în care o trimiteți chiar dumneavoastră, cui nu trebuie.

Evaluări

27. **N3** Când o prelucrare nouă prezintă un risc ridicat pentru persoane, faceți evaluarea impactului prevăzută la art. 35 înainte să începeți. Dacă riscul rămâne ridicat și după măsurile pe care le puteți lua, consultați CNPDCP, conform art. 36.

7. Situații practice

Faceți o instruire și strângeți înscrierile printr-un formular Google.

- **Ce faci:** ceri doar ce folosești, de regulă nume, email și organizație. Pui nota de informare din Anexa 2 în descrierea formularului. Treci activitatea în evidență, cu temei, loc de stocare și termen de păstrare. După instruire, ștergi ce nu îți mai trebuie.
- **Ce NU faci:** nu ceri IDNP-ul, data nașterii sau adresa pentru o simplă înscriere.
- **Cine decide:** coordonatorul de proiect, cu evidența ținută de responsabilul de date.

Ați făcut fotografii la un eveniment și vreți să le publicați pe pagina organizației.

- **Ce faci:** verifici dacă ai acordul pentru publicare, nu doar pentru raportare. Dacă apar copii, verifici acordul reprezentantului legal. Dacă nu ai acordul, publici fotografii de ansamblu în care oamenii nu sunt identificabili.
- **Ce NU faci:** nu tratezi prezența la eveniment ca pe un acord de publicare, și nu te bazezi pe un anunț citit la microfon.
- **Cine decide:** responsabilul de date, împreună cu cine se ocupă de comunicare.

Finanțatorul cere lista participanților, cu nume și date de contact.

- **Ce faci:** verifici ce anume cere contractul de finanțare. Trimiți minimul care satisface cerința. Treci transmiterea în evidență, la rubrica destinatari. Dacă informarea inițială nu spunea că datele merg la finanțator, o completezi pentru viitor.
- **Ce NU faci:** nu trimiți tabelul întreg pentru că e mai simplu decât să faci unul redus.
- **Cine decide:** conducerea, dacă cererea depășește ce ați anunțat participanților.

Un beneficiar vă cere să îi ștergeți datele.

- **Ce faci:** verifici identitatea. Verifici dacă ai o obligație legală sau contractuală de a păstra datele, de exemplu un termen contabil sau o cerință a finanțatorului. Ștergi ce poți șterge, explici în scris ce ești obligat să păstrezi și până când. Răspunzi în cel mult o lună.
- **Ce NU faci:** nu ignori cererea pentru că pare complicată, și nu ștergi documente pe care legea îți cere să le păstrezi.
- **Cine decide:** responsabilul de date.

S-a pierdut un laptop pe care era lista de beneficiari.

- **Ce faci:** anunți responsabilul de date în aceeași zi. Stabiliți împreună ce date erau pe el și dacă erau protejate. Dacă discul era criptat și parola nu e cunoscută altcuiva, riscul e scăzut. Dacă nu, notificați CNPDCP în 72 de ore de când ați aflat, și anunțați persoanele dacă riscul pentru ele e ridicat. Consemnați în registrul de incidente.
- **Ce NU faci:** nu aștepți să afli exact ce s-a întâmplat înainte să pornești termenul de 72 de ore, fiindcă termenul curge deja.
- **Cine decide:** conducerea, la propunerea responsabilului de date.

O autoritate vă cere date despre beneficiari.

- **Ce faci:** ceri cererea în scris, cu temeiul legal invocat. Verifici dacă temeiul acoperă ce se cere. Transmiți doar ce e acoperit. Consemnezi cererea și răspunsul.
- **Ce NU faci:** nu transmiți date pe baza unui telefon și nu transmiți mai mult decât acoperă cererea.
- **Cine decide:** conducerea.

Proiectul s-a încheiat. Ce faceți cu datele adunate în el?

- **Ce faci:** te uiți în evidență la termenele de păstrare. Păstrezi ce cer finanțatorul și legislația contabilă, de regulă cinci ani după plata finală în proiectele europene. Ștergi restul. Consemnezi ce ai șters și când.
- **Ce NU faci:** nu lași dosarul proiectului să rămână în drive „până se face ordine”, și nu ștergi documente justificative înainte de termenul cerut de finanțator.
- **Cine decide:** coordonatorul de proiect, cu responsabilul de date.

8. Excepții, abateri și escaladare

O abatere de la regulile de mai sus poate fi aprobată doar de conducere, pentru o perioadă determinată și cu motivul scris în registrul de incidente și excepții. O excepție fără termen devine practică, iar practica devine regula reală a organizației.

Când o regulă a fost încălcată, prima grijă e limitarea pagubei, nu stabilirea vinovăției. Persoana care semnalează o greșeală proprie nu e sancționată pentru că a semnalat-o. O organizație în care oamenii ascund incidentele află despre ele de la altcineva, de obicei prea târziu ca să mai poată face ceva.

9. Checklist

Periodic

- ☐ Trimestrial: evidența din Anexa 1 e la zi și reflectă activitățile curente.
- ☐ Trimestrial: verificat cine are acces la fișierele cu date despre beneficiari.
- ☐ Anual: termenele de păstrare au expirat undeva? Dacă da, s-a șters?
- ☐ Anual: documentul acesta mai descrie ce faceți în realitate?

Declanșat de eveniment

- ☐ Începe un proiect nou: activitățile lui de prelucrare intră în evidență.
- ☐ Se lansează un formular nou: are nota de informare.
- ☐ Vine un om nou: i se explică regulile și primește doar accesele de care are nevoie.
- ☐ Pleacă un om: i se retrag accesele la fișierele cu date personale.
- ☐ Se încheie un proiect: se aplică termenele de păstrare.
- ☐ S-a produs un incident: termenul de 72 de ore a pornit.

10. Anexe și modele

Anexa 1. Evidența activităților de prelucrare. Se livrează separat, în format Excel și CSV. Cerută de art. 30. Se completează o dată și se actualizează la fiecare activitate nouă.

Anexa 2. Model de informare a persoanei vizate. Se pune în formulare, la înscrieri și oriunde colectați date direct de la om.

[NUMELE ORGANIZAȚIEI] prelucrează datele pe care ni le furnizați (nume, email, organizație) pentru a vă înscrie și a vă contacta în legătură cu [ACTIVITATEA]. Temeiul este [TEMEIUL]. Păstrăm datele [TERMENUL], după care le ștergem. Datele pot fi transmise [DESTINATARI, dacă există]. Aveți dreptul să ne cereți ce date avem despre dumneavoastră, să le corectați, să le ștergeți sau să vă opuneți prelucrării. Ne scrieți la [EMAIL]. Vă puteți adresa și Centrului Național pentru Protecția Datelor cu Caracter Personal.

Anexa 3. Model de consimțământ. Se folosește doar când temeiul chiar este consimțământul.

Sunt de acord ca [NUMELE ORGANIZAȚIEI] să îmi prelucreze datele [CATEGORIILE] în scopul [SCOPUL]. Știu că îmi pot retrage acordul oricând, scriind la [EMAIL], și că retragerea nu afectează prelucrarea de dinainte.

Nume: [.....] Data: [.....] Semnătura: [.....]

Anexa 4. Acord pentru fotografii și înregistrări video. Separat de consimțământul pentru prelucrarea datelor de înscriere, fiindcă acoperă altceva.

Sunt de acord ca [NUMELE ORGANIZAȚIEI] să facă fotografii și înregistrări video la [EVENIMENTUL] în care apar și să le folosească pentru:

- ☐ raportare către finanțator
- ☐ publicare pe paginile și site-ul organizației
- ☐ materiale de informare și promovare

Bifez doar ce accept. Îmi pot retrage acordul scriind la [EMAIL], pentru utilizările viitoare.

Nume: [.....] Data: [.....] Semnătura: [.....]

Pentru participanți sub 18 ani, se completează de reprezentantul legal.

11. Revizuire și versionare

Documentul se revizuieste anual. Se revizuieste și în afara calendarului dacă se schimbă legislația, dacă s-a produs un incident, sau dacă s-a schimbat echipa care lucrează cu datele.

Versiunea	Data	Ce s-a schimbat	Aprobat de
1.0	[DATA]	Versiunea inițială, adoptată din Digital Civic Kit	[ORGANUL CARE APROBĂ]

Digital Civic Kit, elaborat în cadrul proiectului CivicLink Moldova, implementat de Fundația „Laboratorul de Inițiative pentru Dezvoltare” (LID Moldova) în parteneriat cu People in Need Moldova, cu finanțarea Uniunii Europene.

Drepturile asupra Digital Civic Kit aparțin LID Moldova. Organizațiile participante în proiect au dreptul de a utiliza și adapta acest document pentru uz intern, fără drept de comercializare, sublicențiere sau redistribuire către terți ca produs propriu.

Politica de utilizare a instrumentelor digitale și management al conturilor

Documentul 1 din Digital Civic Kit · versiunea 1.0

Acesta este un document-model. Nu produce efecte în organizația dumneavoastră până nu îl adaptați și nu îl aprobați intern. Câmpurile marcate **[ASTFEL]** trebuie completate.

Fișa de adoptare

Câmp	De completat
Organizația	[NUMELE ORGANIZAȚIEI]
Documentul	Politica de utilizare a instrumentelor digitale și management al conturilor
Versiunea	1.0
Aprobat de	[ORGANUL CARE APROBĂ]
Data aprobării	[DATA]
Responsabil	[FUNCȚIA SAU PERSOANA]
Următoarea revizuire	[DATA]
Înlocuiește	[DOCUMENT ANTERIOR] sau „nimic”

0. Cum folosiți acest document

Citiți secțiunile 1 și 2, ca să știți ce acoperă. Completați fișa de adoptare. Parcurgeți regulile din secțiunea 6 și aplicați-le pe cele marcate N1. Aprobați documentul în organul care ia deciziile la dumneavoastră. Reveniți la el la data pe care ați scris-o în fișă.

Fiecare regulă poartă un nivel:

Nivel	Cui i se aplică
N1	Orice organizație, indiferent de mărime. Nu costă bani și nu cere pe cineva tehnic.
N2	Organizații de la 5 oameni în sus, sau care gestionează date ale beneficiarilor.
N3	Proiecte mari, date sensibile, expunere publică ridicată.

Dacă sunteți la început, aplicați N1 în întregime înainte să vă uitați la N2. Un document aplicat pe jumătate corect e mai bun decât unul citit în întregime și neaplicat.

1. Scop și rezultat așteptat

Organizația funcționează pe conturi: email, drive, pagina de Facebook, contul de la bancă, platforma de newsletter, contul de la finanțator. Fiecare are un proprietar, o parolă și un set de oameni care intră în el. Când asta nu e scris nicăieri, organizația nu știe de fapt ce deține, iar accesul se pierde exact în momentul în care e cel mai greu de recuperat: când pleacă omul care îl avea.

Problema nu e teoretică. Cea mai frecventă avarie într-un OSC mic nu e o parolă slabă. E că persoana care a plecat acum doi ani e încă administratorul paginii de Facebook, iar acum nimeni nu poate să publice, să răspundă la mesaje sau să recupereze contul.

Rezultatul așteptat: aveți o listă a conturilor organizației, știți cine intră în fiecare, și când pleacă cineva îi rețineți accesul în aceeași săptămână, dintr-o listă, nu din memorie.

2. Domeniu de aplicare

Se aplică tuturor conturilor folosite pentru activitatea organizației, indiferent cine le-a creat și pe ce adresă sunt înregistrate. Se aplică tuturor persoanelor care le folosesc: angajați, voluntari, membri ai organelor de conducere, stagiați și contractori. Se aplică și dispozitivelor personale, atunci când pe ele se lucrează pentru organizație.

Nu acoperă:

- ce faceți când un cont a fost compromis sau ați pierdut un dispozitiv, tratate în documentul 2 din kit;
- regulile privind datele personale din conturi, tratate în documentul 3;
- accesul la serviciile publice digitale și împuternicirile de reprezentare, tratate în documentul 6.

3. Definiții

Cont instituțional. Cont înregistrat pe o adresă a organizației, deținut de organizație. Rămâne al ei când omul care îl folosea pleacă.

Cont personal folosit în muncă. Cont pe numele unei persoane, folosit pentru treburile organizației. Pleacă odată cu omul.

Cont partajat. Cont folosit de mai multe persoane cu aceeași parolă. Nu se poate ști cine ce a făcut în el.

Administrator. Cel care poate adăuga și scoate alți oameni dintr-un cont sau dintr-o pagină. Nu e același lucru cu cel care o folosește zilnic.

Autentificare în doi pași. Pe lângă parolă, o a doua confirmare, de regulă un cod din telefon. Se mai numește 2FA sau verificare în două etape.

Contact de recuperare. Adresa de email sau numărul de telefon la care serviciul trimite codul când ai uitat parola. Cine controlează contactul de recuperare controlează contul.

Inventar de conturi. Lista conturilor organizației, cu proprietar, administratori și stare. Anexa 1 a acestui document.

Predarea acceselor. Procedura prin care organizația își recuperează conturile de la cineva care pleacă.

4. Cadrul de referință

Legislația Republicii Moldova

- **Legea nr. 195 din 25 iulie 2024 privind protecția datelor cu caracter personal**, publicată în Monitorul Oficial al Republicii Moldova nr. 367-369 din 23 august 2024, art. 574, în vigoare din 23 august 2026. Articolul 32 cere măsuri de securitate potrivite pentru conturile care conțin date despre oameni.
- **Codul muncii al Republicii Moldova**, pentru regulile privind folosirea dispozitivelor personale în muncă și limitele monitorizării angajaților.

Repere europene și internaționale

- **CIS Controls v8.1, Implementation Group 1**, publicate de Center for Internet Security. IG1 este definit ca setul minim de igienă cibernetică pentru organizații fără personal tehnic dedicat. Controalele 1 și 2 acoperă inventarul echipamentelor și al programelor, controlul 5 managementul conturilor, controlul 6 drepturile de acces. Nivelul N1 din acest document e construit pe IG1.
- **ISO/IEC 27001:2022, Anexa A**, controalele A.5.9 (inventarul activelor), A.5.15-A.5.18 (controlul accesului, identitatea, autentificarea, drepturile de acces) și A.8.1 (dispozitivele utilizatorilor).
- **ENISA** (Agenția Uniunii Europene pentru Securitate Cibernetică), *Cybersecurity guide for SMEs*, ghid gratuit în douăsprezece pași pentru organizații mici.

5. Roluri și responsabilități

Rolul	Ce ține	Cine e la dumneavoastră
Responsabil de conturi	Ține inventarul din Anexa 1, dă și retrage accese	[NUME]
Conducerea	Aprobă cine primește drepturi de administrator, aprobă excepțiile	[NUME]
Cine primește un om nou	Parcurge checklistul de venire din Anexa 3	[NUME]
Fiecare membru al echipei	Folosește conturile după regulile de mai jos	toți

Într-o organizație de trei oameni, rolurile de mai sus se comasează. Scrieți în dreptul fiecăruia numele persoanei care îl ține, chiar dacă e aceeași persoană de patru ori.

Un lucru care nu se comasează: **nu lăsați o singură persoană să fie singurul administrator al unui cont important.** Dacă acea persoană nu răspunde la telefon, organizația nu are cont.

6. Reguli și proceduri

Ce conturi aveți

1. **N1** Completați inventarul conturilor din Anexa 1. Treceți tot ce folosiți pentru organizație, inclusiv conturile create demult de cineva care nu mai e în echipă.
2. **N1** Fiecare cont din inventar are un proprietar scris și cel puțin un administrator.
3. **N1** Completați și inventarul dispozitivelor din Anexa 2, cu cine folosește fiecare echipament și dacă pe el sunt date ale organizației.
4. **N2** Revizuiți inventarul trimestrial. Un inventar făcut o dată și uitat descrie organizația de acum un an.

Instituțional și personal

5. **N1** Conturile principale ale organizației se înregistrează pe adrese instituționale, nu pe adresa personală a cuiva. Dacă un cont important e acum pe o adresă personală, treceți-l în inventar și planificați mutarea.
6. **N1** Nu folosiți adresa personală pentru corespondența oficială a organizației. Când omul pleacă, corespondența pleacă cu el, iar organizația nu mai poate dovedi ce a trimis.
7. **N2** Prezența publică a organizației se ține separat de cea personală. O pagină de organizație administrată dintr-un cont personal depinde de acel cont.

Cine intră unde

8. **N1** Accesul se dă după sarcină, nu după funcție sau vechime. Cine nu are nevoie de un cont pentru munca lui nu primește acces la el.
9. **N1** Drepturile de administrator le au cel puțin două persoane și cel mult atâtea cât e nevoie. Una singură e un risc, toată lumea e altul.
10. **N2** Evitați conturile partajate cu aceeași parolă. Unde platforma permite conturi separate, folosiți-le, ca să se poată vedea cine ce a făcut.
11. **N2** Unde un cont partajat nu poate fi evitat, treceți-l ca atare în inventar și schimbați parola când pleacă cineva care o știa.

Parole și autentificare

12. **N1** Fiecare cont are parola lui. O parolă refolosită înseamnă că, scăpată într-un loc, deschide toate celelalte.
13. **N1** Activați autentificarea în doi pași pe conturile importante: email, drive, pagini de social media, bancă. E gratuită la toate serviciile uzuale.
14. **N1** Parolele nu se transmit prin mesaje și nu se țin într-un fișier numit „parole” în drive-ul comun.
15. **N2** Folosiți un gestionar de parole pentru echipă. Există variante gratuite; alegeți una și treceți-o în inventar ca instrument aprobat.

Contactele de recuperare

16. **N1** Contactul de recuperare al unui cont al organizației nu e adresa sau telefonul unei singure persoane care poate pleca. Puneți o adresă instituțională la care au acces cel puțin două persoane.
17. **N1** Verificați contactele de recuperare la fiecare revizuire a inventarului. Un contact de recuperare rămas pe numărul unui fost coleg e o ușă din spate pe care nu o controlați.
18. **N2** Codurile de rezervă oferite de servicii se păstrează undeva unde le găsiți fără contul respectiv, fiindcă exact atunci veți avea nevoie de ele.

Când vine cineva

19. **N1** Parcurgeți checklistul de venire din Anexa 3: ce conturi primește, cu ce drepturi, și cine i-a explicat regulile.
20. **N1** Consemnați în inventar accesele acordate, în ziua în care le-ați acordat.

Când pleacă cineva

21. **N1** Parcurgeți checklistul de plecare din Anexa 3 **în prima săptămână** de la plecare, nu când vă amintiți. Retrageți accesele, schimbați parolele conturilor partajate pe care le știa, mutați drepturile de administrator pe care le deținea.
22. **N1** Verificați dacă persoana era contact de recuperare pentru vreun cont și schimbați contactul înainte să îi închideți adresa.
23. **N1** Recuperați dispozitivele organizației și consemnați predarea în Anexa 2.
24. **N2** Cereți transferul fișierelor de lucru din spațiul personal în cel al organizației înainte de ultima zi, nu după.
25. **N2** Închideți contul instituțional al persoanei sau transformați-l în cutie de corespondență redirectionată, în loc să îl lăsați activ pe termen nedefinit.

Dispozitive

26. **N1** Pe orice dispozitiv pe care se lucrează pentru organizație se pune un cod de acces sau o parolă. Un telefon fără cod e o cheie lăsată în ușă.
27. **N2** Dispozitivele pe care sunt date despre beneficiari se criptează. La telefoanele și laptopurile moderne criptarea e o setare, nu un program de cumpărat.
28. **N2** Programele și sistemele de operare se actualizează. O actualizare amânată luni întregi e cea mai ieftină breșă pe care o puteți lăsa deschisă.

Instrumente

29. **N1** Instrumentele noi folosite pentru munca organizației se trec în inventar. Nu trebuie aprobare pentru fiecare, dar trebuie să se știe ce se folosește.
30. **N3** Înainte să puneți date despre beneficiari într-un instrument nou, verificați unde le stochează și cine mai are acces la ele. Vezi și documentul 3.

7. Situații practice

A plecat colega care ținea pagina de Facebook și nimeni nu mai poate publica.

- **Ce faci:** verifici în inventar cine mai are rol de administrator. Dacă nu mai are nimeni, folosești procedura de recuperare a platformei, care cere de regulă un act de identitate și dovada legăturii cu organizația. Pregătește-te că durează. După ce recuperezi, adaugi imediat un al doilea administrator.
- **Ce NU faci:** nu creezi o pagină nouă. Pierzi urmăritorii, istoricul și dovada că pagina e a organizației.
- **Cine decide:** conducerea, fiindcă recuperarea cere documente ale organizației.

Un voluntar cere acces la drive-ul cu documentele proiectului.

- **Ce faci:** te uiți la ce anume are nevoie pentru sarcina lui și îi dai acces la folderul acela, nu la tot drive-ul. Consemnezi accesul în inventar, cu data.
- **Ce NU faci:** nu îi dai drepturi de administrator ca să nu îl mai deranjezi cu cereri.
- **Cine decide:** responsabilul de conturi.

Contul de email al organizației e înregistrat pe adresa personală a directorului.

- **Ce faci:** treci situația în inventar ca atare. Creezi o adresă instituțională, o pui ca proprietar și contact de recuperare, apoi muți conturile pe ea, unul câte unul, începând cu cele de la care nu vă permiteți să pierdeți accesul.
- **Ce NU faci:** nu amâni până când directorul pleacă. Atunci mutarea nu mai e o operațiune de administrare, ci o negociere.
- **Cine decide:** conducerea.

Cineva vrea să lucreze de pe laptopul personal.

- **Ce faci:** e în regulă, dacă laptopul are parolă la pornire, sistemul e actualizat, iar fișierele organizației stau în spațiul comun, nu doar local. Treci dispozitivul în Anexa 2.
- **Ce NU faci:** nu ceri cuiva să folosească un echipament pe care organizația nu i l-a dat, fără să spui ce condiții se aplică.
- **Cine decide:** responsabilul de conturi, cu acordul persoanei.

S-a terminat proiectul și rămân conturile create pentru el.

- **Ce faci:** te uiți în inventar la ce s-a creat pentru proiect. Ce nu mai e folosit se închide. Ce rămâne primește un proprietar din echipa curentă. Ce conține date despre beneficiari intră sub regulile din documentul 3.
- **Ce NU faci:** nu lași conturile deschise „în caz că”. Un cont pe care nu îl folosește nimeni e un cont pe care nu îl verifică nimeni.
- **Cine decide:** coordonatorul de proiect, cu responsabilul de conturi.

Un finanțator vă cere acces la un dosar din drive.

- **Ce faci:** dai acces la folderul cerut, cu drept de vizualizare, și pui o dată de expirare dacă platforma permite. Consemnezi în inventar cui ai dat acces și pentru ce.
- **Ce NU faci:** nu faci folderul public prin link, ca să fie mai simplu. Un link public circulă mai departe decât credeți.
- **Cine decide:** coordonatorul de proiect.

8. Excepții, abateri și escaladare

O abatere de la regulile de mai sus poate fi aprobată doar de conducere, pentru o perioadă determinată, cu motivul consemnat în inventar. Cea mai frecventă excepție reală e un cont important rămas pe o adresă personală; e acceptabil ca situație temporară, cu termen scris, și inacceptabil ca stare permanentă.

Când cineva își dă seama că a greșit, de exemplu a trimis o parolă pe chat, prima grijă e schimbarea parolei, nu discuția despre cine e de vină.

9. Checklist

Periodic

- ☐ Trimestrial: inventarul conturilor e la zi și fiecare cont are proprietar.
- ☐ Trimestrial: contactele de recuperare sunt instituționale, nu personale.
- ☐ Trimestrial: fiecare cont important are cel puțin doi administratori.
- ☐ Anual: mai folosim toate conturile din inventar? Ce nu se folosește se închide.
- ☐ Anual: documentul acesta mai descrie ce faceți în realitate?

Declanșat de eveniment

- ☐ Vine un om nou: checklistul de venire din Anexa 3, accesele consemnate.
- ☐ Pleacă un om: checklistul de plecare din Anexa 3, în prima săptămână.
- ☐ Se creează un cont nou: intră în inventar în aceeași zi.
- ☐ Începe un proiect: ce conturi îi trebuie și cine le ține.
- ☐ Se încheie un proiect: ce se închide și ce rămâne.

10. Anexe și modele

Anexa 1. Inventarul conturilor și instrumentelor. Se livrează separat, în format Excel și CSV. Coloanele minime sunt marcate cu (*).

Anexa 2. Inventarul dispozitivelor. Idem. Se actualizează la predarea sau primirea unui echipament.

Anexa 3. Checklist la venirea și la plecarea unui om. Se livrează ca fișă tipăribilă, pentru că se folosește în ziua respectivă, nu se citește pe ecran.

La venire: conturile de care are nevoie, cu ce drepturi · autentificarea în doi pași activată · regulile explicate și cine i le-a explicat · dispozitivul predat și consemnat · accesele trecute în inventar.

La plecare, în prima săptămână: accesele retrase, cont cu cont din inventar · parolele conturilor partajate pe care le știa, schimbate · drepturile de administrator mutate pe altcineva · contactele de recuperare pe care figura, schimbate · fișierele de lucru mutate în spațiul organizației · dispozitivele recuperate și consemnate · contul instituțional închis sau redirectionat · data și cine a făcut verificarea.

11. Revizuire și versionare

Documentul se revizuieste anual. Se revizuieste și în afara calendarului dacă se schimbă echipa, dacă ați adoptat un instrument nou important, sau după un incident.

Versiunea	Data	Ce s-a schimbat	Aprobat de
1.0	[DATA]	Versiunea inițială, adoptată din Digital Civic Kit	[ORGANUL CARE APROBĂ]

Digital Civic Kit, elaborat în cadrul proiectului CivicLink Moldova, implementat de Fundația „Laboratorul de Inițiative pentru Dezvoltare” (LID Moldova) în parteneriat cu People in Need Moldova, cu finanțarea Uniunii Europene.

Drepturile asupra Digital Civic Kit aparțin LID Moldova. Organizațiile participante în proiect au dreptul de a utiliza și adapta acest document pentru uz intern, fără drept de comercializare, sublicențiere sau redistribuire către terți ca produs propriu.

Politica de securitate digitală și răspuns la incidente

Documentul 2 din Digital Civic Kit · versiunea 1.0

Acesta este un document-model. Nu produce efecte în organizația dumneavoastră până nu îl adaptați și nu îl aprobați intern. Câmpurile marcate **[ASTFEL]** trebuie completate.

Fișa de adoptare

Câmp	De completat
Organizația	[NUMELE ORGANIZAȚIEI]
Documentul	Politica de securitate digitală și răspuns la incidente
Versiunea	1.0
Aprobat de	[ORGANUL CARE APROBĂ]
Data aprobării	[DATA]
Responsabil	[FUNCȚIA SAU PERSOANA]
Următoarea revizuire	[DATA]
Înlocuiește	[DOCUMENT ANTERIOR] sau „nimic”

0. Cum folosiți acest document

Citiți secțiunile 1 și 2, ca să știți ce acoperă. Completați fișa de adoptare. Parcurgeți regulile din secțiunea 6 și aplicați-le pe cele marcate N1. Tipăriți fișa de triaj din Anexa 1 și puneți-o unde o găsiți repede. Aprobați documentul în organul care ia deciziile la dumneavoastră.

Fiecare regulă poartă un nivel:

Nivel	Cui i se aplică
N1	Orice organizație, indiferent de mărime. Nu costă bani și nu cere pe cineva tehnic.
N2	Organizații de la 5 oameni în sus, sau care gestionează date ale beneficiarilor.
N3	Proiecte mari, date sensibile, expunere publică ridicată.

1. Scop și rezultat așteptat

Documentul răspunde la o singură întrebare, în două momente diferite. Ce facem ca să nu se întâmple, și ce facem în primele ore după ce s-a întâmplat.

Partea a doua contează mai mult decât pare. O organizație care nu a trecut niciodată printr-un incident nu are de unde ști ce face în ziua în care contul e preluat sau laptopul dispare, iar atunci nu e momentul să afle. Aici sunt scrise pașii dinainte, ca să nu fie improvizați atunci.

Rezultatul așteptat: oricine din echipă știe pe cine sună în prima oră după ce ceva merge prost, fără să caute și fără să întrebe.

2. Domeniu de aplicare

Se aplică tuturor persoanelor care lucrează în numele organizației și tuturor conturilor și dispozitivelor folosite pentru activitatea ei. Acoperă atât incidentele tehnice, cât și atacurile îndreptate împotriva oamenilor din organizație.

Nu acoperă:

- inventarul conturilor și predarea acceselor, tratate în documentul 1;
- obligațiile legale privind datele personale în ansamblu, tratate în documentul 3. Aici e doar partea de notificare a unei încălcări.

3. Definiții

Incident. Orice situație în care conturile, dispozitivele, datele sau oamenii organizației sunt afectați: cont preluat, dispozitiv pierdut, date ajunse unde nu trebuie, atac asupra unei persoane din echipă.

Phishing. Mesaj care imită o sursă de încredere ca să vă smulgă parola sau un cod. Poate veni pe email, pe mesagerie sau prin telefon.

Preluarea contului. Situația în care altcineva intră în contul organizației sau al unei persoane și îl controlează.

Doxxing. Publicarea datelor personale ale cuiva, de regulă adresă, telefon sau date despre familie, cu scopul de a-l expune la hărțuire.

Copie de rezervă. O a doua copie a fișierelor, într-un loc separat, din care puteți restaura dacă originalul e pierdut sau blocat.

CNPDCP. Centrul Național pentru Protecția Datelor cu Caracter Personal, autoritatea de supraveghere pentru datele personale (datepersonale.md).

ASC. Agenția pentru Securitate Cibernetică, autoritatea națională în domeniul securității cibernetice (ncsc.md).

4. Cadrul de referință

Legislația Republicii Moldova

- **Legea nr. 195 din 25 iulie 2024 privind protecția datelor cu caracter personal**, publicată în Monitorul Oficial nr. 367-369 din 23 august 2024, art. 574, în vigoare din 23 august 2026. Articolul 32 cere măsuri de securitate; **articolul 33 cere notificarea CNPDCP în cel mult 72 de ore** atunci când o încălcare prezintă un risc pentru persoane; articolul 34 cere anunțarea persoanelor afectate când riscul e ridicat.
- **Legea nr. 48/2023 privind securitatea cibernetică**, care armonizează parțial cadrul național cu Directiva (UE) 2022/2555. Atenție la domeniul ei de aplicare: obligațiile de notificare din articolul 12 revin entităților aflate în sfera legii, adică furnizorilor de servicii esențiale și entităților publice. **O organizație a societății civile obișnuită nu intră în această categorie**, deci nu are obligația legală de a notifica un incident cibernetic. Poate însă notifica voluntar, iar în multe cazuri merită.

Repere europene și internaționale

- **Directiva (UE) 2022/2555**, cunoscută ca NIS2, articolul 21, cele zece măsuri de gestionare a riscurilor. Nu vi se aplică direct, dar e standardul după care se orientează statul, deci e o listă bună de verificat.
- **Digital First Aid Kit**, dezvoltat de Digital Defenders Partnership împreună cu Rapid Response Network și CiviCERT. Trasee de prim ajutor pas cu pas pentru incidente, construite pentru societatea civilă, gratuite și în mai multe limbi (digitalfirstaid.org).
- **SAFETAG**, cadru de audit de securitate organizațională dezvoltat de Internews pentru organizații mici care apără drepturi.
- **Access Now Digital Security Helpline**, linie de asistență pentru organizații ale societății civile, disponibilă permanent și în mai multe limbi.
- **Ghidul de securitate digitală pentru ONG-uri** publicat de Asociația TechSoup România împreună cu ApTI, gratuit și în limba română. Igiena tehnică de bază din secțiunea 6 e

compatibilă cu lista lor de verificare; unde vreți mai mult detaliu tehnic, mergeți acolo.

- **NIST SP 800-63B-4** (august 2025), pentru recomandarea privind frazele-parolă lungi în locul parolelor scurte și complicate.

5. Roluri și responsabilități

Rolul	Ce ține	Cine e la dumneavoastră
Responsabil de incidente	Primește semnalările, pornește fișa de triaj, ține registrul	[NUME]
Conducerea	Decide notificările, vorbește în numele organizației, aprobă excepțiile	[NUME]
Cine se ocupă de comunicare	Aplică planul din Anexa 3 când incidentul devine public	[NUME]
Fiecare membru al echipei	Semnaleză imediat, fără să aștepte confirmarea	toți

Într-o organizație de trei oameni, rolurile de mai sus se comasează. Scrieți în dreptul fiecăruia numele persoanei care îl ține, chiar dacă e aceeași persoană de patru ori.

6. Reguli și proceduri

Igiena de bază

Regulile de aici sunt minimul. Pentru detalii tehnice mai ample există ghidul gratuit în limba română al Asociației TechSoup România și ApTI, citat în secțiunea 4; nu îl repetăm.

1. **N1** Fiecare cont are parola lui, lungă și diferită de celelalte. O frază de patru cuvinte e mai greu de spart și mai ușor de ținut minte decât o parolă scurtă cu simboluri.
2. **N1** Autentificarea în doi pași e activată pe email, drive, pagini de social media și bancă. E gratuită peste tot unde contează.
3. **N1** Sistemele și aplicațiile se actualizează. Actualizările închid exact ușile pe care intră atacurile automate.
4. **N1** Există o copie de rezervă a fișierelor importante, în alt loc decât originalul, și ați verificat cel puțin o dată că se poate restaura din ea. O copie netestată e o presupunere.
5. **N1** Pe rețele Wi-Fi publice nu vă autentificați în conturile organizației, decât dacă folosiți o conexiune securizată.
6. **N2** Documentele sensibile stau în spații cu acces limitat, nu în foldere deschise întregii echipe.

Recunoașterea încercărilor de fraudă

7. **N1** Nu introduceți parola într-o pagină la care ați ajuns dintr-un link primit prin mesaj. Deschideți serviciul separat și intrați ca de obicei.
8. **N1** Niciun serviciu legitim nu vă cere codul de verificare în doi pași prin telefon sau mesaj. Cine îl cere, îl fură.
9. **N1** O cerere urgentă de plată sau de transfer, venită prin email de la conducere, se verifică pe alt canal înainte de a fi executată, chiar dacă adresa pare corectă.
10. **N2** Cine primește un mesaj suspect îl semnalează echipei, nu doar îl șterge. Același mesaj ajunge de obicei la mai mulți.

Securitatea oamenilor, nu doar a conturilor

Secțiunea aceasta acoperă atacurile îndreptate spre persoane, nu spre sisteme. Ele nu se rezolvă cu parole și sunt, pentru o organizație vizibilă, mai probabile decât o spargere tehnică.

11. **N1** Persoanele expuse public din organizație își verifică ce date despre ele sunt accesibile: adresă, telefon, informații despre familie, locuri frecventate. Ce nu e necesar public se retrage.
12. **N1** Când cineva din echipă primește amenințări sau e ținta unei campanii de hărțuire, anunță imediat conducerea. Nu e o problemă personală pe care o duce singur.
13. **N1** Nu răspundeți public atacatorilor și nu intrați în polemică. Salvați dovezile: capturi de ecran cu data vizibilă, linkuri, nume de conturi.
14. **N1** Raportați conținutul pe platforma pe care apare și, dacă există amenințări la adresa persoanei, la poliție. O amenințare nu devine mai puțin reală pentru că e scrisă pe internet.

15. **N2** Organizația asigură sprijin juridic și, la cerere, psihologic persoanei vizate. Costul de a nu face asta se plătește în oameni care pleacă.
16. **N2** Când atacul vizează organizația ca întreg, aplicați planul de comunicare din Anexa 3: cine vorbește, ce spunem, ce nu facem.
17. **N3** Organizațiile cu expunere publică ridicată stabilesc dinainte un canal alternativ de comunicare internă, pentru cazul în care cel obișnuit e compromis.

Când s-a întâmplat ceva

18. **N1** Orice suspiciune se anunță responsabilului de incidente în aceeași zi. Nu așteptați să fiți siguri. Un semnal fals costă zece minute; o oră pierdută la un incident real costă mult mai mult.
19. **N1** Primul pas e limitarea pagubei: schimbați parola, deconectați sesiunile active, scoateți dispozitivul din rețea. Abia apoi începe lămurirea a ce s-a întâmplat.
20. **N1** Deschideți fișa de triaj din Anexa 1 și mergeți pe ea. E scrisă ca să fie urmată de cineva agitat.
21. **N1 Dacă sunt implicate date despre oameni, termenul de 72 de ore din articolul 33 a pornit deja**, din momentul în care ați aflat, nu din momentul în care veți înțelege ce s-a întâmplat. Notificarea se face și cu informații incomplete și se completează ulterior.
22. **N2** Fiecare incident se consemnează în registrul din Anexa 2, inclusiv cele pe care ați decis să nu le notificați, cu motivul deciziei.
23. **N2** După fiecare incident, o discuție scurtă despre ce se schimbă ca să nu se repete. Un incident din care nu se schimbă nimic se va repeta.

Pregătirea

24. **N1** Fișa de triaj e tipărită și accesibilă fără cont și fără internet. Dacă e doar în drive, exact în ziua în care vă trebuie s-ar putea să nu o puteți deschide.
25. **N2** O dată pe an, parcurgeți în echipă un scenariu: contul de Facebook a fost preluat. Cincisprezece minute de exercițiu valorează mai mult decât documentul necitit.
26. **N3** Organizațiile cu risc ridicat pot cere un audit de securitate după cadrul SAFETAG, construit pentru organizații ca ale dumneavoastră.

7. Situații practice

Pagina de Facebook a organizației a fost preluată.

- **Ce faci:** verifici dacă mai ai acces din alt cont de administrator. Schimbi parola contului personal al administratorului, care e de regulă calea de intrare, și deconectezi sesiunile active. Folosești procedura de recuperare a platformei. Anunți public de pe alt canal al organizației că pagina e compromisă, ca să nu creadă lumea mesajele publicate de pe ea. Consemnezi în registru.
- **Ce NU faci:** nu creezi imediat o pagină nouă și nu negociezi cu cine a preluat-o.
- **Cine decide:** conducerea, împreună cu responsabilul de incidente.

Cineva din echipă a dat parola pe o pagină falsă.

- **Ce faci:** schimbi imediat parola contului respectiv și a oricărui alt cont unde parola era refolosită. Deconectezi sesiunile active. Activezi autentificarea în doi pași dacă nu era. Verifici dacă s-au trimis mesaje din cont și dacă au fost adăugate reguli de redirecționare a emailului, care e o urmă frecventă și ușor de ratat. Verifici dacă în cont erau date despre oameni, fiindcă atunci intră în discuție termenul de 72 de ore.
- **Ce NU faci:** nu tratezi omul ca pe vinovat. Data viitoare nu va mai spune.
- **Cine decide:** responsabilul de incidente.

S-a pierdut un laptop pe care erau documente ale organizației.

- **Ce faci:** stabilești ce era pe el și dacă discul era criptat. Schimbi parolele conturilor la care laptopul era conectat. Dacă erau date despre oameni și discul nu era criptat, mergi pe traseul de notificare. Consemnezi în registru și în inventarul de dispozitive din documentul 1.
- **Ce NU faci:** nu presupui că parola de la Windows protejează fișierele. Fără criptare, nu le protejează.
- **Cine decide:** conducerea, la propunerea responsabilului de incidente.

O colegă primește amenințări online după o postare a organizației.

- **Ce faci:** o întrebi întâi ce are nevoie. Salvați dovezile împreună, cu data vizibilă. Raportați conținutul pe platformă. Dacă sunt amenințări la adresa persoanei, mergeți la poliție. Organizația preia comunicarea publică, nu o lasă pe ea să răspundă singură. Oferi sprijin juridic și, dacă vrea, psihologic.
- **Ce NU faci:** nu îi ceri să ignore și să treacă peste. Nu răspunzi public atacatorilor.
- **Cine decide:** conducerea, dar felul în care se comunică se decide împreună cu persoana vizată.

Apare o campanie coordonată împotriva organizației.

- **Ce faci:** deschizi planul din Anexa 3. Stabilești cine vorbește, un singur om. Verifici ce anume se afirmă și dacă e ceva ce trebuie corectat factual. Anunți partenerii și finanțatorul înainte să afle din altă parte. Documentezi.
- **Ce NU faci:** nu răspunzi la fiecare mesaj și nu intri în ritmul impus de campanie.
- **Cine decide:** conducerea.

Un mesaj de la „directorul executiv” cere urgent o plată către un cont nou.

- **Ce faci:** îl suni pe director la numărul pe care îl știi, nu la cel din mesaj. Dacă plata a fost deja făcută, anunți imediat banca; șansele de recuperare scad cu fiecare oră. Anunți poliția. Consemnezi.
- **Ce NU faci:** nu execuți plata pentru că mesajul pare urgent. Urgența e instrumentul.
- **Cine decide:** conducerea.

Fișierele de pe un calculator s-au blocat și se cere răscumpărare.

- **Ce faci:** deconectezi calculatorul de la rețea și de la orice disc extern, ca să nu se întindă. Verifici copia de rezervă. Restaurezi pe un sistem curat. Anunți poliția. Dacă erau date despre oameni, intră în discuție notificarea.

- **Ce NU faci:** nu plătești răscumpărarea. Nu garantează nimic și vă marchează ca țintă care plătește.
- **Cine decide:** conducerea.

8. Excepții, abateri și escaladare

Nu există excepție de la regula de a semnală. Orice altă regulă poate fi suspendată temporar de conducere, cu motivul consemnat.

Într-un incident, ierarhia se scurtează: cine observă are dreptul să ia primele măsuri de limitare, chiar dacă nu găsește pe nimeni. E mai bine să schimbați o parolă fără aprobare decât să așteptați aprobarea.

Persoana care semnalează propria greșeală nu e sancționată pentru semnalare. O organizație în care oamenii ascund incidentele află despre ele de la altcineva, de obicei prea târziu.

9. Checklist

Periodic

- ☐ Lunar: copiile de rezervă s-au făcut și s-a testat restaurarea din ele.
- ☐ Trimestrial: autentificarea în doi pași e activă pe toate conturile importante.
- ☐ Trimestrial: sistemele și aplicațiile sunt actualizate.
- ☐ Anual: fișa de triaj e tipărită, la zi și cu numerele corecte.
- ☐ Anual: un exercițiu de cincisprezece minute pe un scenariu.
- ☐ Anual: documentul acesta mai descrie ce faceți în realitate?

Declanșat de eveniment

- ☐ S-a semnalat ceva: fișa de triaj deschisă, ora consemnată.
- ☐ Sunt implicate date personale: termenul de 72 de ore a pornit.
- ☐ Incidentul s-a închis: consemnat în registru, cu ce s-a schimbat după.
- ☐ Pleacă un om: vezi documentul 1, secțiunea de plecare.

10. Anexe și modele

Anexa 1. Fișa de triaj: pe cine suni, în ce ordine. Se livrează ca fișă A4 tipăribilă. Structura:

Întâi, în primele minute: limitează. Schimbă parola, deconectează sesiunile, scoate dispozitivul din rețea. Notează ora.

Apoi, în funcție de ce s-a întâmplat:

Sunt implicate date despre oameni? → CNPDCP, în cel mult 72 de ore de când ai aflat. Obligație legală, articolul 33 din Legea nr. 195/2024. Dacă riscul pentru persoane e ridicat, anunță și persoanele.

Incident cibernetic, fără date personale? → Agenția pentru Securitate Cibernetică, ncsc.md. Pentru o organizație a societății civile obișnuită **nu e obligatoriu**, fiindcă obligația din Legea nr. 48/2023 revine entităților din sfera ei. Notificarea voluntară rămâne utilă: primești sprijin și contribuiți la imaginea de ansamblu.

Fraudă, furt de bani, șantaj? → poliția. Dacă s-a făcut o plată, întâi banca, în aceeași oră.

Atac asupra unei persoane din echipă? → platforma pe care apare, poliția dacă sunt amenințări, și sprijin juridic. Vezi și Anexa 3.

Nu știi în ce categorie intră? → digitalfirstaid.org, trasee pas cu pas, gratuit. Sau Access Now Digital Security Helpline, pentru organizații ale societății civile.

Contacte proprii, de completat: responsabil de incidente [NUME, TELEFON] · conducere [NUME, TELEFON] · bancă [TELEFON] · jurist [NUME, TELEFON].

Anexa 2. Registrul incidentelor. Se livrează separat, în format Excel și CSV. Se consemnează și incidentele nenotificate, cu motivul.

Anexa 3. Plan de comunicare de criză. Se livrează ca fișă A4 tipăribilă. Se completează înainte de a fi nevoie de el, nu în ziua în care e nevoie.

Cine vorbește. O singură persoană vorbește public: [NUME, FUNCȚIE]. Înlocuitor, dacă prima nu e disponibilă în două ore: [NUME, FUNCȚIE]. Restul echipei trimite întrebările către ea și nu comentează public, nici de pe conturile personale.

Pe cine anunțăm, în ordinea asta. Întâi echipa, ca să nu afle din altă parte. Apoi persoanele afectate, dacă sunt. Apoi finanțatorul, dacă incidentul atinge date sau bani din proiect. Apoi publicul, dacă e cazul. Autoritățile merg în paralel, pe traseul din Anexa 1, nu după ce am terminat de comunicat.

Ce spunem în primul mesaj. Ce s-a întâmplat, în două propoziții, fără termeni tehnici. Ce am făcut deja. Ce nu știm încă și când revenim cu detalii. Un mesaj scurt și onest, publicat repede, e mai bun decât unul complet publicat peste trei zile.

Ce nu facem. Nu spunem „totul e sub control” înainte să știm că este. Nu dăm vina pe un om din echipă. Nu intrăm în polemică și nu răspundem atacatorilor. Nu ștergem postări sau mesaje care există deja public, fiindcă ștergerea devine ea însăși subiect. Nu promitem un termen pe care nu îl putem ține.

Contacte externe, de completat: poliție [TELEFON] · bancă [TELEFON] · jurist [NUME, TELEFON] · sprijin psihologic [NUME, TELEFON] · finanțator [NUME, EMAIL] · persoana care administrează site-ul și paginile [NUME, TELEFON].

După ce s-a încheiat. Cine scrie ce s-a întâmplat, în registrul din Anexa 2, și în cât timp: [NUME], în [NUMĂRI] zile.

Anexa 4. Checklist periodic de securitate. Se livrează ca fișă A4 tipăribilă. Se bifează la datele din stânga și se păstrează bifată, ca să se vadă când s-a făcut ultima dată.

Lunar

- ☐ Copiile de rezervă s-au făcut, și s-a restaurat un fișier din ele ca probă.
- ☐ Nu au rămas conturi active ale unor oameni care au plecat.

Trimestrial

- ☐ Autentificarea în doi pași e activă pe email, drive, pagini și bancă.
- ☐ Sistemele, aplicațiile și telefoanele de serviciu sunt actualizate.
- ☐ Contactele de recuperare ale conturilor sunt adrese instituționale, nu personale.
- ☐ Cine are acces la fișierele cu date despre beneficiari mai are nevoie de el.

Anual

- ☐ Fișa de triaj e tipărită, la zi, cu numerele corecte, și știe echipa unde stă.
- ☐ Planul de comunicare de criză are numele și numerele actuale.
- ☐ Un exercițiu de cincisprezece minute pe un scenariu, cu toată echipa.
- ☐ Documentul acesta mai descrie ce faceți în realitate.

Data ultimei verificări: [DATA] · **cine a făcut-o:** [NUME]

11. Revizuire și versionare

Documentul se revizuieste anual. Se revizuieste și după fiecare incident, fiindcă atunci aflați ce lipsea din el.

Versiunea	Data	Ce s-a schimbat	Aprobat de
1.0	[DATA]	Versiunea inițială, adoptată din Digital Civic Kit	[ORGANUL CARE APROBĂ]

Digital Civic Kit, elaborat în cadrul proiectului CivicLink Moldova, implementat de Fundația „Laboratorul de Inițiative pentru Dezvoltare” (LID Moldova) în parteneriat cu People in Need Moldova, cu finanțarea Uniunii Europene.

Drepturile asupra Digital Civic Kit aparțin LID Moldova. Organizațiile participante în proiect au dreptul de a utiliza și adapta acest document pentru uz intern, fără drept de comercializare, sublicențiere sau redistribuire către terți ca produs propriu.

Procedură de management digital al proiectelor, documentelor și datelor

Documentul 5 din Digital Civic Kit · versiunea 1.0

Acesta este un document-model. Nu produce efecte în organizația dumneavoastră până nu îl adaptați și nu îl aprobați intern. Câmpurile marcate **[ASTFEL]** trebuie completate.

Fișa de adoptare

Câmp	De completat
Organizația	[NUMELE ORGANIZAȚIEI]
Documentul	Procedură de management digital al proiectelor, documentelor și datelor
Versiunea	1.0
Aprobat de	[ORGANUL CARE APROBĂ]
Data aprobării	[DATA]
Responsabil	[FUNCȚIA SAU PERSOANA]
Următoarea revizuire	[DATA]
Înlocuiește	[DOCUMENT ANTERIOR] sau „nimic”

0. Cum folosiți acest document

Citiți secțiunile 1 și 2, ca să știți ce acoperă. Completați fișa de adoptare. Parcurgeți regulile din secțiunea 6 și aplicați-le pe cele marcate N1. Aplicați structura de foldere din Anexa 1 la următorul proiect care începe, nu retroactiv la toate.

Fiecare regulă poartă un nivel:

Nivel	Cui i se aplică
N1	Orice organizație, indiferent de mărime. Nu costă bani și nu cere pe cineva tehnic.
N2	Organizații de la 5 oameni în sus, sau care gestionează date ale beneficiarilor.
N3	Proiecte mari, date sensibile, expunere publică ridicată.

1. Scop și rezultat așteptat

Un proiect produce, în doi ani, câteva sute de fișiere: contracte, rapoarte, liste de participanți, poze, facturi, tabele cu indicatori. Dacă nu au un loc și un nume, ele există doar în memoria celui care le-a făcut. Când vine auditul, când pleacă omul, sau când finanțatorul cere ceva la trei ani după închidere, organizația caută în loc să găsească.

Documentul stabilește unde stau documentele unui proiect, cum se numesc, cine le ține la zi, cât se păstrează și ce se face la închidere.

Rezultatul așteptat: oricine din echipă găsește un document al unui proiect încheiat în sub cinci minute, fără să întrebe pe cel care l-a făcut.

2. Domeniu de aplicare

Se aplică documentelor și datelor produse în proiectele organizației, indiferent de finanțator, și documentelor administrative care le însoțesc. Se aplică tuturor persoanelor care lucrează în proiecte.

Nu acoperă:

- regulile privind datele cu caracter personal, tratate în documentul 3. Aici e doar unde stau și cât se păstrează;
- conturile și accesele la spațiile de stocare, tratate în documentul 1;
- raportarea către stat și depunerea documentelor oficiale, tratate în documentul 6.

3. Definiții

Spațiu comun. Locul unde stau documentele organizației și la care au acces cei care au nevoie. Un drive al organizației, nu drive-ul personal al cuiva.

Versiune. O stare a unui document la un moment dat. Versionarea înseamnă să știi care e ultima și cine a schimbat ce.

Arhivare. Mutarea documentelor unui proiect încheiat într-un loc unde nu se mai modifică, dar se pot găsi.

Termen de păstrare. Perioada în care sunteți obligați să păstrați un document, dată de finanțator sau de lege.

Indicator. O mărime pe care o raportați finanțatorului, de exemplu numărul de participanți la instruirii.

Document justificativ. Actul care dovedește o cheltuială sau o activitate: factură, listă de prezență, contract.

4. Cadrul de referință

Legislația Republicii Moldova

- **Legea nr. 86/2020 cu privire la organizațiile necomerciale.** Raportul anual de activitate se face public în termen de șase luni de la încheierea anului la care se referă; dacă nu e publicat, se transmite oricui îl solicită în termen de o lună. Modificările de statut, sediu, adresă electronică sau organe de conducere se comunică organului de înregistrare de stat în termen de trei luni.
- Termenele de păstrare din legislația contabilă și arhivistică, pentru documentele justificative.

Repere europene și internaționale

- **PM²**, metodologia de management de proiect a Comisiei Europene, în ediția deschisă, publicată gratuit împreună cu peste treizeci de modele de documente. Structura de foldere și logica de denumire din anexele acestui document sunt adaptate din ea. E util să știți asta când discutați cu un finanțator european: nu e o convenție inventată de noi.
- **ISO 15489**, standardul pentru managementul înregistrărilor.
- **Principiile FAIR** pentru datele de cercetare și de proiect: să poată fi găsite, accesate, folosite împreună cu altele și reutilizate.
- **Cerințele finanțatorilor.** Acordurile de grant ale Uniunii Europene cer, ca regulă, păstrarea documentelor justificative timp de cinci ani după plata finală. Verificați în contractul dumneavoastră, fiindcă termenul poate fi mai lung.

5. Roluri și responsabilități

Rolul	Ce ține	Cine e la dumneavoastră
Coordonator de proiect	Structura folderelor proiectului, registrul, închiderea	[NUME]
Responsabil administrativ	Documentele justificative și termenele de păstrare	[NUME]
Conducerea	Aprobă structura, decide ce se arhivează și ce se șterge	[NUME]
Fiecare membru al echipei	Salvează în spațiul comun, după regulile de denumire	toți

Într-o organizație de trei oameni, rolurile de mai sus se comasează. Scrieți în dreptul fiecăruia numele persoanei care îl ține, chiar dacă e aceeași persoană de patru ori.

6. Reguli și proceduri

Unde stau documentele

1. **N1** Documentele proiectelor stau în spațiul comun al organizației, nu în spațiul personal al cuiva și nu doar pe laptopul cuiva. Un fișier care există într-un singur loc, pe un singur calculator, e un fișier pe cale să se piardă.
2. **N1** Fiecare proiect are un folder propriu, cu structura din Anexa 1. Structura se creează la începutul proiectului, nu când începe raportarea.
3. **N1** Ce e în lucru și ce e final se ține separat. Un folder **final** în care intră doar versiunile trimise scutește de întrebarea „pe care am trimis-o?”.
4. **N2** Documentele care conțin date despre beneficiari stau într-un subfolder cu acces limitat, nu în folderul deschis întregii echipe. Vezi documentul 3.

Cum se numesc

5. **N1** Fișierele se numesc după regula din Anexa 2: dată, proiect, tip, versiune. Numele se citește fără să deschizi fișierul.
6. **N1** Data se scrie în format an-lună-zi, de exemplu **2026-09-08**. Așa fișierele se ordonează singure cronologic.
7. **N1** Fără diacritice, spații și semne speciale în numele fișierelor. Se folosesc cratime. Un nume cu diacritice poate deveni ilizibil când fișierul trece prin alt sistem sau e trimis unui finanțator.
8. **N1** Nu folosiți **final**, **final2**, **final-bun** ca versionare. Folosiți **v1**, **v2**, **v3**.

Versiuni

9. **N1** Când modificați un document deja trimis, salvați o versiune nouă. Nu suprascrieți ce a plecat din organizație.
10. **N2** Unde platforma păstrează istoricul versiunilor, folosiți-l în loc să faceți copii. Cinci copii ale aceluiași document sunt cinci ocazii de a lucra pe cea greșită.
11. **N2** Documentele semnate se păstrează ca atare, în formatul în care au fost semnate, și nu se mai editează.

Lucrul împreună

12. **N1** Se lucrează pe fișierul din spațiul comun, nu pe copii trimise prin email. Un document trimis ca atașament devine imediat două documente diferite.
13. **N2** Sarcinile proiectului se țin într-un loc vizibil întregii echipe, oricare ar fi acesta. Un tabel comun e suficient; nu vă trebuie o platformă plătită.
14. **N2** Termenele care implică mai mulți oameni stau într-un calendar comun.

Datele proiectului

15. **N1** Datele colectate în proiect, de exemplu listele de participanți, se strâng într-un singur loc, nu în câte un tabel per activitate.

16. **N1** Indicatorii pe care îi raportați finanțatorului se actualizează pe parcurs, nu se reconstituie la final. Reconstituirea la final e momentul în care se descoperă că lipsesc listele de prezență.
17. **N2** Cine colectează datele știe de la început ce se raportează din ele. O rubrică lipsă într-un formular de înscriere se plătește cu o lună de căutări.
18. **N2** Datele care conțin informații despre oameni intră și în evidența din documentul 3.

Cât se păstrează

19. **N1** Fiecare proiect are scris în registru termenul de păstrare a documentelor, luat din contractul de finanțare. Când contractul spune cinci ani după plata finală, termenul curge de la plata finală, nu de la încheierea activităților.
20. **N1** Nu ștergeți documente justificative înainte de termenul din contract, chiar dacă proiectul pare demult închis.
21. **N2** Când termenul a expirat, ștergeți ce nu mai trebuie păstrat, mai ales datele despre oameni. Păstrarea la nesfârșit nu e prudentă, e o obligație pe care v-o luați singuri.

Închiderea

22. **N1** La încheierea proiectului parcurgeți checklistul din Anexa 4. Închiderea se face când echipa își mai amintește proiectul, nu peste un an.
23. **N1** Consemnați în registrul din Anexa 3 unde a rămas arhiva proiectului și cine răspunde de ea.
24. **N2** Scrieți o pagină cu ce a mers și ce nu. E singurul moment în care informația aceasta e încă disponibilă și e ce vă va lipsi la scrierea următoarei cereri de finanțare.

7. Situații practice

Începe un proiect nou.

- **Ce faci:** creezi folderul cu structura din Anexa 1. Îl treci în registrul din Anexa 3, cu finanțator, perioadă și termen de păstrare luat din contract. Stabilești cine are acces la subfolderul cu date despre beneficiari. Deschizi tabelul de indicatori.
- **Ce NU faci:** nu începi cu un folder gol numit după proiect, în care se adaugă fișiere pe măsură ce apar.
- **Cine decide:** coordonatorul de proiect.

Trebuie trimis raportul intermediar și nu se găsesc listele de prezență de la două instruirii.

- **Ce faci:** cauți în folderul activității respective și la persoana care a ținut instruirea. Dacă listele nu există, consemnezi asta onest și explici cum reconstitui numărul, de exemplu din înscrieri și fotografii. Apoi schimbi procesul: lista se scanează și se urcă în aceeași zi cu activitatea.
- **Ce NU faci:** nu completezi retroactiv o listă de prezență. E un document justificativ, iar reconstituirea lui e altceva decât falsificarea lui.
- **Cine decide:** coordonatorul de proiect, cu responsabilul administrativ.

Doi oameni au lucrat pe versiuni diferite ale aceluiași raport.

- **Ce faci:** stabilești care e ultima versiune reală, după dată și după cine a lucrat ultimul. Compari și integrezi. Salvezi rezultatul ca versiune nouă, în spațiul comun, și ștergi copiile locale.
- **Ce NU faci:** nu alegi versiunea celui care insistă mai mult.
- **Cine decide:** coordonatorul de proiect.

Finanțatorul cere, la doi ani după închidere, documente dintr-un proiect.

- **Ce faci:** te uiți în registru unde a rămas arhiva. Scoți ce se cere. Dacă lipsește ceva, spui ce lipsește și de ce, în loc să amâni răspunsul.
- **Ce NU faci:** nu cauți prin drive-urile personale ale foștilor colegi. Dacă acolo ajungi, problema e la închidere, nu la căutare.
- **Cine decide:** responsabilul administrativ.

Un coleg pleacă în mijlocul proiectului.

- **Ce faci:** înainte de ultima zi, muți fișierele lui de lucru în spațiul comun și treci în registru ce rămâne neterminat. Vezi și documentul 1 pentru accese.
- **Ce NU faci:** nu presupui că tot ce a lucrat e deja în spațiul comun. De regulă nu e.
- **Cine decide:** coordonatorul de proiect.

Proiectul s-a încheiat și folderul are opt sute de fișiere.

- **Ce faci:** parcurgi checklistul din Anexa 4. Muți documentele finale și justificative în arhivă. Ștergi versiunile intermediare care nu mai au rost. Aplici termenele de păstrare pentru datele despre oameni, din documentul 3. Consemnezi în registru.
- **Ce NU faci:** nu arhivezi tot, ca să fii sigur. O arhivă în care e totul e o arhivă în care nu găsești nimic, și păstrează date personale fără temei.
- **Cine decide:** coordonatorul de proiect, cu conducerea.

8. Excepții, abateri și escaladare

Structura de foldere se adaptează la proiect, dar nu se abandonează pentru un proiect anume fiindcă „e mic”. Proiectele mici sunt exact cele ale căror documente se pierd.

Termenele de păstrare nu admit excepții interne. Sunt luate din contracte și din lege, iar organizația nu le poate scurta prin decizie proprie.

Când o regulă a fost încălcată și un document s-a pierdut, se consemnează pierderea și ce se schimbă. Un document pierdut și nedeclarat devine o problemă la audit, unde costă mai mult.

9. Checklist

Periodic

- ☐ Lunar: indicatorii proiectelor active sunt actualizați.
- ☐ Trimestrial: documentele din spațiile personale s-au mutat în cel comun.
- ☐ Anual: raportul de activitate a fost publicat în termenul din Legea nr. 86/2020.

- ☐ Anual: termenele de păstrare au expirat undeva? Dacă da, s-a șters?
- ☐ Anual: documentul acesta mai descrie ce faceți în realitate?

Declanșat de eveniment

- ☐ Începe un proiect: folder creat cu structura, proiect trecut în registru.
- ☐ Se semnează un contract: salvat în folderul lui, în formatul semnat.
- ☐ Are loc o activitate: lista de prezență scanată și urcată în aceeași zi.
- ☐ Pleacă un om: fișierele lui de lucru mutate în spațiul comun.
- ☐ Se încheie un proiect: checklistul de închidere din Anexa 4.

10. Anexe și modele

Anexa 1. Structura-model de foldere pentru un proiect. Adaptată din PM². Se copiază la începutul fiecărui proiect.

AAAA-nume-proiect/ **01-contract-si-finantare/** contractul, actele adiționale, bugetul aprobat
02-planificare/ planul de activități, calendarul, bugetul de lucru **03-activitati/** un subfolder per activitate, cu materialele ei **04-participanti/ acces limitat.** Înscrieri, liste de prezență, acorduri **05-financiar/** facturi, plăți, documente justificative **06-raportare/** rapoarte intermediare și final, cu indicatorii **07-comunicare/** materiale, fotografii, postări **08-final/** doar versiunile trimise și acceptate **09-arhiva/** se creează la închidere

Anexa 2. Reguli de denumire și versionare.

AAAA-LL-ZZ_proiect_tip-document_vN.extensie

Exemple: **2026-09-08_civiclink_raport-intermediar_v2.docx** ·
2026-09-08_civiclink_lista-prezenta-cahul_v1.pdf

Fără diacritice, fără spații, fără **final**. Data în față, ca ordonarea să fie cronologică.

Anexa 3. Registrul proiectelor și al arhivării. Se livrează separat, în format Excel și CSV. Conține finanțator, perioadă, unde stau documentele, responsabil de arhivare și termenul de păstrare cu sursa lui.

Anexa 4. Checklist de închidere și arhivare a unui proiect. Fișă tipăribilă.

Raportul final trimis și acceptat · documentele justificative complete în **05-financiar** · indicatorii finali consemnați · versiunile trimise mutate în **08-final** · versiunile intermediare fără rost, șterse · datele despre participanți tratate după termenele din documentul 3 · arhiva creată și locul ei trecut în registru · responsabilul de arhivă numit · pagina cu ce a mers și ce nu, scrisă · accesele la folderul proiectului, revizuite.

11. Revizuire și versionare

Documentul se revizuieste anual. Se revizuieste și în afara calendarului dacă schimbați spațiul de stocare sau dacă un finanțator nou cere altă structură de raportare.

Versiunea	Data	Ce s-a schimbat	Aprobat de
1.0	[DATA]	Versiunea inițială, adoptată din Digital Civic Kit	[ORGANUL CARE APROBĂ]

Digital Civic Kit, elaborat în cadrul proiectului CivicLink Moldova, implementat de Fundația „Laboratorul de Inițiative pentru Dezvoltare” (LID Moldova) în parteneriat cu People in Need Moldova, cu finanțarea Uniunii Europene.

Drepturile asupra Digital Civic Kit aparțin LID Moldova. Organizațiile participante în proiect au dreptul de a utiliza și adapta acest document pentru uz intern, fără drept de comercializare, sublicențiere sau redistribuire către terți ca produs propriu.

Politica privind utilizarea responsabilă a inteligenței artificiale

Documentul 4 din Digital Civic Kit · versiunea 1.0

Acesta este un document-model. Nu produce efecte în organizația dumneavoastră până nu îl adaptați și nu îl aprobați intern. Câmpurile marcate **[ASTFEL]** trebuie completate.

Fișa de adoptare

Câmp	De completat
Organizația	[NUMELE ORGANIZAȚIEI]
Documentul	Politica privind utilizarea responsabilă a inteligenței artificiale
Versiunea	1.0
Aprobat de	[ORGANUL CARE APROBĂ]
Data aprobării	[DATA]
Responsabil	[FUNCȚIA SAU PERSOANA]
Următoarea revizuire	[DATA]
Înlocuiește	[DOCUMENT ANTERIOR] sau „nimic”

0. Cum folosiți acest document

Citiți secțiunile 1 și 2, ca să știți ce acoperă. Completați fișa de adoptare. Parcurgeți regulile din secțiunea 6 și aplicați-le pe cele marcate N1. Completați lista de instrumente din Anexa 1 cu ce folosiți deja, nu cu ce ați vrea să folosiți.

Fiecare regulă poartă un nivel:

Nivel	Cui i se aplică
N1	Orice organizație, indiferent de mărime. Nu costă bani și nu cere pe cineva tehnic.
N2	Organizații de la 5 oameni în sus, sau care gestionează date ale beneficiarilor.
N3	Proiecte mari, date sensibile, expunere publică ridicată.

1. Scop și rezultat așteptat

Documentul nu introduce inteligența artificială în organizație. Ea e deja acolo. Oamenii o folosesc ca să redacteze, să traducă, să reformuleze și să rezume, iar asta se întâmplă de regulă fără nicio regulă scrisă, pe conturi personale, cu ce text le vine la îndemână să lipească în ele.

Riscul practic nu e că textul iese prost. E că, într-o zi obișnuită, cineva lipește într-un instrument public o listă de beneficiari, un raport nepublicat sau un document primit de la un partener, ca să îl rezume. Datele acelea au plecat din organizație și nu se mai întorc.

Rezultatul așteptat: oricine din echipă știe, fără să întrebe, ce are voie să introducă într-un instrument de inteligență artificială și ce nu introduce niciodată.

2. Domeniu de aplicare

Se aplică tuturor instrumentelor care generează sau prelucrează text, imagini, sunet ori date în numele organizației, indiferent dacă sunt folosite de pe un cont al organizației sau de pe unul personal, atunci când munca e pentru organizație.

Nu acoperă:

- utilizarea personală, în afara muncii pentru organizație;
- regulile generale privind datele cu caracter personal, tratate în documentul 3. Aici e doar ce nu se introduce în astfel de instrumente;
- funcțiile de inteligență artificială integrate în programe pe care le folosiți oricum, de exemplu corectorul dintr-un editor de text, atâta timp cât nu le trimiteți conținut sensibil.

3. Definiții

Instrument de inteligență artificială. Un serviciu care generează text, imagini, sunet sau analize pe baza a ceea ce îi dați. Exemple uzuale: asistenți conversaționali, generatoare de imagini,

servicii de transcriere a înregistrărilor.

Prompt. Ce îi scrieți instrumentului. Tot ce puneți în prompt pleacă la furnizor.

Rezultat generat. Ce vă întoarce instrumentul. Nu e verificat, nu e o sursă și nu e al dumneavoastră până nu îl verificați și nu vi-l asumați.

Halucinație. Situația în care instrumentul produce o informație plauzibilă și falsă: o lege care nu există, o cifră inventată, o sursă care sună real. Se întâmplă des și arată convingător.

Date confidențiale. Tot ce nu ați publica: date despre beneficiari, documente nepublicate, informații primite de la parteneri, date financiare, corespondență internă.

Deepfake. Conținut generat care imită vocea, chipul sau stilul unei persoane reale.

4. Cadrul de referință

Un lucru de spus de la început. Republica Moldova nu are, la data acestui document, o lege proprie privind inteligența artificială. Reperele de mai jos nu se aplică direct aici. Le folosim pentru că sunt cea mai bună practică disponibilă și pentru că indică direcția spre care se îndreaptă reglementarea, inclusiv la noi.

Repere europene și internaționale

- **Regulamentul (UE) 2024/1689 privind inteligența artificială.** Trei părți din el sunt utile unei organizații ca a dumneavoastră:
 - **articolul 5** enumeră practicile interzise, iar ele formează coloana „Interzis” din Anexa 1 fără să fie nevoie să o inventăm;
 - **articolul 50** cere ca un text generat cu inteligență artificială și publicat pentru a informa publicul asupra unor chestiuni de interes public să fie declarat ca atare. E articolul care cade cel mai direct pe comunicarea publică a unei organizații de advocacy;
 - **articolul 4** cere ca oamenii care folosesc astfel de sisteme să aibă un nivel suficient de competență în domeniu. E motivul pentru care o politică singură nu ajunge, și trebuie dublată de o discuție în echipă.
- **ALTAI**, lista de autoevaluare pentru o inteligență artificială demnă de încredere, elaborată de grupul de experți la nivel înalt al Comisiei Europene, structurată pe șapte cerințe. Checklistul din Anexa 2 e o formă redusă a ei.
- **Convenția-cadru a Consiliului Europei privind inteligența artificială și drepturile omului, democrația și statul de drept**, semnată de Republica Moldova la 5 septembrie 2024, la Vilnius.
- **Recomandarea UNESCO privind etica inteligenței artificiale.**

Legislația Republicii Moldova care se aplică oricum

- **Legea nr. 195 din 25 iulie 2024 privind protecția datelor cu caracter personal**, publicată în Monitorul Oficial nr. 367-369 din 23 august 2024, art. 574. Nu vorbește despre inteligență artificială, dar se aplică integral: a lipi date despre oameni într-un instrument public este o prelucrare, și încă una prin care datele ajung la un terț.

Notă de transparență. Persoana care a elaborat acest document este membru al Consiliului Național pentru Inteligența Artificială în Educație de pe lângă Ministerul Educației și Cercetării. E o poziție instituțională într-un domeniu pe care documentul îl tratează, și preferăm să o știți.

5. Roluri și responsabilități

Rolul	Ce ține	Cine e la dumneavoastră
Responsabil de instrumente	Ține lista din Anexa 1, aprobă instrumente noi	[NUME]
Conducerea	Aprobă politica, decide în cazurile neclare	[NUME]
Cine publică	Aplică checklistul din Anexa 2 înainte de publicare	[NUME]
Fiecare membru al echipei	Răspunde de ce trimite mai departe, generat sau nu	toți

Într-o organizație de trei oameni, rolurile de mai sus se comasează. Scrieți în dreptul fiecăruia numele persoanei care îl ține, chiar dacă e aceeași persoană de patru ori.

Regula care nu se deleagă: responsabilitatea pentru un text rămâne a omului care îl semnează sau îl trimite. Instrumentul nu răspunde de nimic.

6. Reguli și proceduri

Ce nu se introduce niciodată

1. **N1** Nu introduceți date despre persoane identificabile: nume, contacte, liste de participanți, date despre beneficiari, informații despre starea lor. Dacă aveți nevoie de ajutor cu un text care le conține, scoateți-le întâi.
2. **N1** Nu introduceți documente nepublicate ale organizației: cereri de finanțare în lucru, rapoarte nedepuse, procese-verbale, corespondență internă.
3. **N1** Nu introduceți documente primite de la parteneri, finanțatori sau beneficiari. Nu sunt ale dumneavoastră ca să le dați mai departe.
4. **N1** Nu introduceți date financiare, contracte sau informații despre salarii.
5. **N2** Nu introduceți informații care ar putea expune o persoană la risc, chiar dacă nu o numesc direct. Într-o comunitate mică, un detaliu de context identifică omul.

Ce se poate face

6. **N1** Se poate folosi pentru: redactarea și reformularea unui text public, traducere, rezumarea unui document public, generarea de idei, ordonarea propriilor notițe, explicarea unui concept.
7. **N1** Se poate folosi pentru a îmbunătăți un text pe care l-ați scris dumneavoastră. Se folosește cu prudență pentru a scrie de la zero un text pe care nu îl puteți verifica.

Ce instrumente

8. **N1** Completați lista din Anexa 1 cu instrumentele pe care echipa le folosește deja. Începeți de la realitate, nu de la o listă ideală.
9. **N1** Fiecare instrument din listă are un statut: **Permis**, **Cu precauție** sau **Interzis**, și un rând care spune pentru ce anume.
10. **N2** Un instrument nou se trece în listă înainte să fie folosit pentru muncă. Nu e nevoie de o procedură lungă; e nevoie să se știe.
11. **N2** Verificați, înainte să aprobați un instrument, dacă furnizorul folosește ce introduceți pentru antrenarea modelelor și dacă se poate dezactiva. La multe servicii există o setare pentru asta.
12. **N3** Pentru date sensibile, dacă nu găsiți un instrument cu garanții suficiente, răspunsul corect e să nu îl folosiți pentru acele date.

Verificarea rezultatului

13. **N1** Orice rezultat generat se verifică înainte de a fi folosit. Instrumentele produc cu egală siguranță informații corecte și informații inventate.
14. **N1** Cifrele, citatele, numele de instituții, articolele de lege și sursele se verifică la sursa originală, întotdeauna. O trimitere la un act normativ generată automat se confruntă cu textul actului, fiindcă numerele de articole sunt exact genul de detaliu pe care instrumentele îl greșesc convingător.

15. **N1** Nu preluați un rezultat pe care nu îl puteți explica cuiva cu cuvintele dumneavoastră. Dacă nu îl puteți explica, nu îl puteți susține.
16. **N2** Parcurgeți checklistul din Anexa 2 înainte să publicați ceva construit cu ajutorul acestor instrumente.

Transparență

17. **N1** Nu prezentați drept muncă proprie un text preluat integral și nemodificat.
18. **N2** Când publicați material de informare pe teme de interes public construit în mod substanțial cu astfel de instrumente, spuneți-o. E cerința articolului 50 din regulamentul european; nu vi se aplică juridic, dar într-un sector care trăiește din credibilitate e exact genul de lucru care se află oricum.
19. **N2** O mențiune scurtă e suficientă. Nu e nevoie de o declarație lungă pentru un text la care instrumentul a ajutat la corectură.

Drepturi și conținut generat

20. **N2** Nu presupuneți că un rezultat generat e liber de drepturi. Verificați condițiile furnizorului înainte să îl folosiți într-un material care se publică sau se distribuie.
21. **N2** Imaginile generate care înfățișează persoane nu se folosesc ca și cum ar fi fotografii reale ale beneficiarilor. Într-un raport, asta e o denaturare.
22. **N3** Conținutul care imită o persoană reală, ca voce sau ca imagine, nu se produce și nu se distribuie. Vezi și documentul 2 pentru situația în care altcineva îl produce despre dumneavoastră.

Oameni

23. **N1** Nicio decizie despre o persoană, de exemplu selecția unui beneficiar sau evaluarea unei cereri, nu se ia automat pe baza unui rezultat generat. Instrumentul poate ajuta la ordonare; decizia o ia un om, care poate explica de ce.
24. **N2** Discutați regulile din acest document în echipă, cel puțin o dată. O politică pe care nimeni nu a citit-o nu schimbă ce se lipește în instrumente.

7. Situații practice

Vreți să rezumați un raport de proiect de patruzeci de pagini.

- **Ce faci:** verifici dacă raportul e public. Dacă e, îl poți rezuma. Dacă nu e, scoți numele, datele de contact și detaliile care identifică oameni, sau rezumi capitol cu capitol fără părțile sensibile.
- **Ce NU faci:** nu urci raportul întreg pentru că e mai rapid.
- **Cine decide:** coordonatorul de proiect.

Trebuie tradus un material pentru beneficiari.

- **Ce faci:** traduci textul, apoi îl citește cineva care știe limba, mai ales dacă materialul conține instrucțiuni pe care oamenii le vor urma. O traducere aproape corectă a unei instrucțiuni e mai periculoasă decât lipsa traducerii.

- **Ce NU faci:** nu publici o traducere pe care nu a citit-o nimeni.
- **Cine decide:** cine răspunde de comunicare.

Un coleg a scris cererea de finanțare cu ajutorul unui instrument și a inclus statistici.

- **Ce faci:** verifici fiecare cifră și fiecare sursă la origine. Cifrele generate arată exact ca cele reale. Ce nu poate fi verificat, se scoate.
- **Ce NU faci:** nu trimiți la finanțator o cifră pe care nu ai găsit-o într-o sursă.
- **Cine decide:** coordonatorul de proiect.

Vreți să transcrieți înregistrarea unui interviu cu un beneficiar.

- **Ce faci:** te oprești. Înregistrarea conține vocea și povestea unei persoane identificabile. Ai nevoie de temei și de informarea persoanei, conform documentului 3, și de un instrument în care ai încredere. Dacă nu le ai pe amândouă, transcrii manual.
- **Ce NU faci:** nu urci înregistrarea într-un serviciu gratuit găsit pe internet.
- **Cine decide:** responsabilul de date, împreună cu conducerea.

Vi se cere o postare pe o temă de interes public și o construieți cu ajutorul unui instrument.

- **Ce faci:** verifici afirmațiile, scrii cu cuvintele organizației, și adaugi o mențiune scurtă despre felul în care a fost pregătit materialul.
- **Ce NU faci:** nu publici un text generat integral, nemodificat, pe o temă unde credibilitatea organizației e miza.
- **Cine decide:** cine răspunde de comunicare.

Un instrument nou apare și toată lumea îl folosește.

- **Ce faci:** îl treci în Anexa 1, verifici ce face cu datele introduse, îi dai un statut și spui echipei pentru ce se poate folosi.
- **Ce NU faci:** nu îl interzici reflex și nu îl accepți reflex.
- **Cine decide:** responsabilul de instrumente.

8. Excepții, abateri și escaladare

Regulile 1-5, despre ce nu se introduce niciodată, nu admit excepții. Datele plecate nu se recuperează, iar o excepție „doar de data asta” e chiar cazul în care se pierde.

Restul regulilor pot fi suspendate temporar de conducere, cu motivul consemnat.

Dacă cineva își dă seama că a introdus ceva ce nu trebuia, anunță imediat. Situația se tratează ca incident, după documentul 2, și, dacă erau date despre oameni, se aplică documentul 3, inclusiv termenul de 72 de ore. Prima grijă e evaluarea a ce a plecat, nu discuția despre cine a greșit.

9. Checklist

Periodic

- ☐ Semestrial: lista din Anexa 1 mai reflectă ce folosește echipa? Instrumentele se schimbă repede.
- ☐ Semestrial: setările de confidențialitate ale instrumentelor aprobate sunt încă active.
- ☐ Anual: o discuție în echipă despre ce a mers și unde au apărut probleme.
- ☐ Anual: documentul acesta mai descrie ce faceți în realitate?

Declanșat de eveniment

- ☐ Apare un instrument nou: trecut în listă, cu statut.
- ☐ Se publică un material construit cu astfel de instrumente: checklistul din Anexa 2.
- ☐ Vine un om nou: i se explică regulile 1-5.
- ☐ S-a introdus ceva ce nu trebuia: tratat ca incident.

10. Anexe și modele

Anexa 1. Instrumente: Permis, Cu precauție, Interzis. Se livrează separat, în format Excel și CSV.
Model de completare:

Instrument	Statut	Pentru ce	Ce nu se introduce niciodată
Asistent conversațional general	Permis	Redactare, reformulare, traducere, idei	Date despre oameni, documente nepublicate
Serviciu de transcriere	Cu precauție	Înregistrări publice, ședințe interne fără date sensibile	Interviuri cu beneficiari
Generator de imagini	Cu precauție	Ilustrații generice	Imagini care par fotografii ale beneficiarilor
Orice instrument neverificat	Interzis	—	—

Anexa 2. Checklist înainte de a folosi un rezultat generat. Fișă tipăribilă, formă redusă a ALTAI.

Înainte să trimiți sau să publici:

- ☐ Am verificat cifrele, citatele și sursele la origine.
- ☐ Am verificat trimiterile la acte normative în textul legii.
- ☐ Pot explica cu cuvintele mele tot ce scrie aici.
- ☐ Nu am introdus date despre persoane, documente nepublicate sau materiale primite de la parteneri.
- ☐ Textul spune ce vrea organizația să spună, nu ce a nimerit instrumentul.
- ☐ Dacă e material public pe temă de interes public, am adăugat mențiunea.
- ☐ Dacă sunt imagini generate, nu pot fi confundate cu fotografii reale.
- ☐ Un om își asumă acest material. Numele lui: **[NUME]**.

11. Revizuire și versionare

Documentul se revizuieste **semestrial**, mai des decât celelalte din kit, fiindcă instrumentele și condițiile lor se schimbă în luni, nu în ani. Se revizuieste și când apare o reglementare națională în domeniu.

Versiunea	Data	Ce s-a schimbat	Aprobat de
1.0	[DATA]	Versiunea inițială, adoptată din Digital Civic Kit	[ORGANUL CARE APROBĂ]

Digital Civic Kit, elaborat în cadrul proiectului CivicLink Moldova, implementat de Fundația „Laboratorul de Inițiative pentru Dezvoltare” (LID Moldova) în parteneriat cu People in Need Moldova, cu finanțarea Uniunii Europene.

Drepturile asupra Digital Civic Kit aparțin LID Moldova. Organizațiile participante în proiect au dreptul de a utiliza și adapta acest document pentru uz intern, fără drept de comercializare, sublicențiere sau redistribuire către terți ca produs propriu.

Ghid practic: serviciile publice digitale și relația digitală cu statul și cu finanțatorii

Documentul 6 din Digital Civic Kit · versiunea 1.0

Acesta este un document-model. Nu produce efecte în organizația dumneavoastră până nu îl adaptați și nu îl aprobați intern. Câmpurile marcate **[ASTFEL]** trebuie completate.

Informațiile despre servicii sunt verificate la 8 septembrie 2026. E documentul din kit care se învechește cel mai repede. Verificați la sursă înainte de a vă baza pe un detaliu.

Fișa de adoptare

Câmp	De completat
Organizația	[NUMELE ORGANIZAȚIEI]
Documentul	Ghid practic: serviciile publice digitale și relația digitală cu statul și cu finanțatorii
Versiunea	1.0
Aprobat de	[ORGANUL CARE APROBĂ]
Data aprobării	[DATA]
Responsabil	[FUNCȚIA SAU PERSOANA]
Următoarea revizuire	[DATA]
Înlocuiește	[DOCUMENT ANTERIOR] sau „nimic”

0. Cum folosiți acest document

Documentul acesta e altfel decât celelalte din kit. Nu vă învață ce e o semnătură electronică, fiindcă o folosiți deja. Începe de la lucrurile pe care organizațiile chiar le greșesc: cine are dreptul să semneze în numele organizației, ce se întâmplă cu acel drept când omul pleacă, și unde ajung notificările oficiale.

Completați registrul din Anexa 1. Parcurgeți regulile din secțiunea 6. Restul e material de referință, de citit când vă trebuie.

Nivel	Cui i se aplică
N1	Orice organizație, indiferent de mărime. Nu costă bani și nu cere pe cineva tehnic.
N2	Organizații de la 5 oameni în sus, sau care gestionează date ale beneficiarilor.
N3	Proiecte mari, date sensibile, expunere publică ridicată.

1. Scop și rezultat așteptat

Organizațiile societății civile din Moldova folosesc deja serviciile publice digitale, și le folosesc mult. Ce lipsește nu e obișnuința, ci evidența: cine deține semnătura electronică a organizației, cine a primit dreptul să o reprezinte, până când, și cine retrage dreptul acela când omul pleacă.

O împrumut electronică rămasă activă pe numele unui fost coleg e mai gravă decât un cont de Facebook uitat. Cu ea se poate semna în numele organizației, în relația cu statul.

Rezultatul așteptat: știți în orice moment cine poate semna și acționa în numele organizației în relația cu statul, și puteți retrage acel drept în aceeași zi în care hotărâți.

2. Domeniu de aplicare

Se aplică tuturor acceselor organizației la servicii publice digitale și tuturor persoanelor care acționează în numele ei în relația cu instituțiile statului.

Nu acoperă:

- conturile și instrumentele obișnuite ale organizației, tratate în documentul 1. Aici sunt doar accesul la serviciile statului;
- obligațiile privind datele cu caracter personal, tratate în documentul 3;
- arhivarea documentelor de proiect, tratată în documentul 5.

3. Definiții

Semnătură electronică calificată. Semnătura care are aceeași valoare juridică cu cea olografă. Se obține de la un prestator acreditat și e legată de o persoană fizică, nu de organizație.

Împuternicire. Dreptul dat unei persoane de a acționa în numele alteia, pentru un scop anume. Se acordă electronic și se poate revoca electronic.

EVO. Portalul guvernamental prin care se accesează serviciile publice, evo.gov.md. Versiunea EVO 2.0 a fost lansată în 2026.

MPower. Registrul împuternicirilor de reprezentare, creat de Agenția de Guvernare Electronică și lansat în noiembrie 2020. Este integrat în EVO, de unde se acordă, se revizuiesc și se revocă împuternicirile.

MSign. Serviciul guvernamental prin care se semnează electronic documentele.

Persoană cu drept de reprezentare. Cine poate acționa în numele organizației potrivit statutului și datelor din registrul de stat, de regulă directorul executiv sau președintele.

4. Cadrul de referință

Legislația Republicii Moldova

- **Legea nr. 91 din 29.05.2014 privind semnătura electronică și documentul electronic.** Stabilește valoarea juridică a semnăturii electronice și condițiile în care un document electronic produce aceleași efecte ca unul pe hârtie.
- **Legea nr. 86/2020 cu privire la organizațiile necomerciale.** Raportul anual de activitate se face public în termen de șase luni de la încheierea anului. Modificările de statut, sediu, adresă electronică sau organe de conducere se comunică organului de înregistrare de stat în termen de trei luni. **Adresa electronică e printre datele care se comunică**, ceea ce nu e evident și se uită des.
- **Legea nr. 195 din 25 iulie 2024 privind protecția datelor cu caracter personal**, publicată în Monitorul Oficial nr. 367-369 din 23 august 2024, art. 574. Se aplică și datelor pe care le transmiteți instituțiilor, și celor pe care le primiți de la ele.

Instituții și servicii

Agenția de Guvernare Electronică (AGE), Serviciul Tehnologie Informației și Securitate Cibernetică (STISC), Agenția Servicii Publice (ASP), Serviciul Fiscal de Stat (SFS), Casa Națională de Asigurări Sociale (CNAS).

Repere europene

- **Regulamentul (UE) nr. 910/2014**, cunoscut ca eIDAS, și **Regulamentul (UE) 2024/1183** care instituie portofelul european de identitate digitală. Republica Moldova își aliniază treptat serviciile la această direcție; EVO 2.0 include deja un portofel de identitate digitală construit în logica standardelor europene.
- **Strategia de transformare digitală a Republicii Moldova 2023-2030.**

5. Roluri și responsabilități

Rolul	Ce ține	Cine e la dumneavoastră
Reprezentant legal	Deține semnătura electronică, acordă și revocă împuterniciri	[NUME]
Responsabil administrativ	Ține registrul din Anexa 1, urmărește termenele de raportare	[NUME]
Contabil, intern sau extern	Raportarea fiscală și socială, în limita împuternicirii primite	[NUME]
Conducerea	Decide cine primește împuterniciri și pe ce durată	[NUME]

Într-o organizație de trei oameni, rolurile de mai sus se comasează. Scrieți în dreptul fiecăruia numele persoanei care îl ține, chiar dacă e aceeași persoană de patru ori.

Atenție la o confuzie frecventă: semnătura electronică aparține unei persoane fizice, nu organizației. Directorul care pleacă pleacă cu semnătura lui. Organizația nu o moștenește.

6. Reguli și proceduri

Evidența acceselor

1. **N1** Completați registrul din Anexa 1: ce servicii folosiți, cine are acces la fiecare, cine deține semnătură electronică și ce împuterniciri sunt active.
2. **N1** Fiecare împuternicire activă are în registru o dată de expirare sau mențiunea că e pe durată nedeterminată. O împuternicire fără termen se revizuieste cel puțin anual.
3. **N2** Revizuiți registrul trimestrial și la fiecare schimbare în echipă.

Semnătura electronică

4. **N1** Cel puțin două persoane din organizație dețin semnătură electronică. Cu una singură, organizația se oprește când acea persoană e bolnavă, plecată sau a demisionat.
5. **N1** Semnătura electronică nu se împrumută. Este legată de o persoană și semnarea cu semnătura altcuiva înseamnă că acea persoană răspunde pentru ce ați semnat.
6. **N1** Urmăriți data de expirare a certificatelor. O semnătură expirată descoperită în ziua unui termen de depunere e o problemă evitabilă.
7. **N2** Când reprezentantul legal se schimbă, actualizați datele la organul de înregistrare de stat înainte să aveți nevoie să semnați ceva important.

Împuterniciri

8. **N1** Împuternicirile se acordă pentru un scop determinat și pentru o durată determinată, nu general și pe termen nelimitat.
9. **N1 Când pleacă un om, împuternicirile lui se revocă în aceeași săptămână**, odată cu celelalte accese din documentul 1. Revocarea se face electronic, de unde a fost acordată.
10. **N1** Consemnați în registru data revocării, nu doar data acordării.
11. **N2** Contabilul extern primește împuternicire pentru raportarea fiscală, nu acces la contul de semnătură al directorului. Sunt lucruri diferite, iar al doilea nu e permis.
12. **N2** Verificați anual lista împuternicirilor active. Este cel mai probabil loc în care găsiți un nume care nu ar trebui să fie acolo.

Notificări și corespondență oficială

13. **N1** Adresa electronică pe care o primesc notificările oficiale este una instituțională, la care au acces cel puțin două persoane, nu adresa personală a directorului.
14. **N1** Cineva verifică notificările oficiale periodic, nu doar când așteaptă ceva. O notificare necitită curge la termen indiferent dacă a fost citită.
15. **N1** Când se schimbă adresa electronică a organizației, se comunică organului de înregistrare de stat, în termenul de trei luni din Legea nr. 86/2020.
16. **N2** Corespondența oficială primită se salvează în spațiul comun, după regulile din documentul 5, nu rămâne doar în cutia poștală a cuiva.

Raportare

17. **N1** Termenele de raportare se trec într-un calendar comun: raportul anual de activitate din Legea nr. 86/2020, raportările fiscale și cele sociale.
18. **N1** Raportul anual de activitate se face public în șase luni de la încheierea anului. Dacă nu îl publicați, sunteți obligați să îl transmiteți oricui îl cere, în termen de o lună, ceea ce e mai multă muncă decât publicarea.
19. **N2** Confirmările de depunere se păstrează. O depunere fără dovadă e, la o verificare, o depunere care nu s-a făcut.

Datele în relația cu statul

20. **N1** Nu transmiteți mai multe date decât cere temeiul invocat de instituție. Vezi documentul 3, situația privind cererile autorităților.
21. **N2** Consemnați ce ați transmis, cui și în ce temei.

7. Situații practice

A plecat directorul și el deținea singura semnătură electronică.

- **Ce faci:** verifici în registru ce împuterniciri erau active pe numele lui și le revoci. Actualizezi datele reprezentantului legal la organul de înregistrare de stat. Noul reprezentant își obține propria semnătură electronică. Până atunci, organizația nu poate semna electronic, deci tratezi asta ca pe o urgență, nu ca pe o formalitate administrativă.
- **Ce NU faci:** nu folosești semnătura fostului director, chiar dacă ți-a lăsat datele de acces. Semnătura e a lui și el rămâne răspunzător pentru ce se semnează cu ea.
- **Cine decide:** conducerea.

Contabilul extern are nevoie să depună rapoartele fiscale.

- **Ce faci:** îi acorzi împuternicire pentru scopul acesta, pe durata contractului, și o treci în registru cu data de expirare. La încetarea contractului, o revoci.
- **Ce NU faci:** nu îi dai datele de acces ale directorului ca să fie mai simplu.
- **Cine decide:** reprezentantul legal.

Nu găsiți o notificare despre care o instituție spune că v-a fost transmisă.

- **Ce faci:** verifici în portal, nu doar în email. Verifici la ce adresă electronică e înregistrată organizația, fiindcă poate fi una veche. Dacă adresa e greșită, o corectezi la organul de înregistrare de stat.
- **Ce NU faci:** nu presupui că lipsa unui email înseamnă lipsa unei notificări. Termenul a curs.
- **Cine decide:** responsabilul administrativ.

Organizația și-a schimbat sediul și adresa electronică.

- **Ce faci:** comunică modificările organului de înregistrare de stat în termen de trei luni, conform Legii nr. 86/2020. Actualizezi adresa în serviciile prin care primiți notificări. Treci în registru ce ai actualizat și când.

- **Ce NU faci:** nu amâni pentru că „oricum ne gălesc”. Modificările necomunicate în termen sunt o problemă la prima verificare.
- **Cine decide:** conducerea.

Un proiect nou cere înregistrarea într-o platformă a unui finanțator.

- **Ce faci:** creezi contul pe o adresă instituțională, nu personală. Îl treci în registrul din Anexa 1 și în inventarul din documentul 1. Stabilești cine îl administrează, minimum două persoane.
- **Ce NU faci:** nu îl creezi pe adresa coordonatorului de proiect, care se va încheia.
- **Cine decide:** coordonatorul de proiect, cu responsabilul administrativ.

Vreți să vedeți ce împuterniciri active are organizația.

- **Ce faci:** intri în EVO, în modulul de împuterniciri, și verifici lista. Compari cu registrul din Anexa 1. Ce e activ și nu ar trebui, revoci. Ce lipsește din registru, adaugi.
- **Ce NU faci:** nu te bazezi doar pe registrul intern. Sursa de adevăr e ce e înregistrat la stat.
- **Cine decide:** responsabilul administrativ.

8. Excepții, abateri și escaladare

Nu există excepție de la regula 5: semnătura electronică nu se împrumută. Consecințele nu sunt administrative, ci personale, pentru cel al cărui certificat a fost folosit.

Restul regulilor pot fi suspendate temporar de conducere, cu motivul consemnat în registru.

9. Checklist

Periodic

- ☐ Trimestrial: registrul din Anexa 1 e la zi.
- ☐ Trimestrial: lista împuternicirilor active din EVO corespunde cu registrul intern.
- ☐ Semestrial: certificatele de semnătură electronică nu expiră în curând.
- ☐ Anual: raportul de activitate a fost publicat în termenul de șase luni.
- ☐ Anual: adresa electronică înregistrată la stat e cea pe care o citiți.

Declanșat de eveniment

- ☐ Pleacă un om: împuternicirile revocate în aceeași săptămână.
- ☐ Se schimbă reprezentantul legal: date actualizate la registrul de stat, semnătură nouă.
- ☐ Se schimbă sediul sau adresa electronică: comunicat în trei luni.
- ☐ Începe un contract cu un contabil extern: împuternicire cu termen.
- ☐ Se încheie acel contract: împuternicire revocată.

10. Anexe și modele

Anexa 1. Registrul acceselor la serviciile de stat. Se livrează separat, în format Excel și CSV. Conține serviciul, cine are acces, tipul de semnătură sau acces, dacă există împuternicire, valabilitatea, data revocării și data ultimei verificări.

Anexa 2. Checklist: semnătura electronică și delegarea prin EVO. Fișă tipăribilă.

Ce verific la fiecare schimbare în echipă:

- ☐ Cine deține semnătură electronică validă în organizație? Sunt cel puțin doi?
- ☐ Ce împuterniciri sunt active în EVO, pe ce nume, până când?
- ☐ Persoana care pleacă figurează în vreo împuternicire? Revocată la data de [.....]
- ☐ Adresa electronică pentru notificări oficiale e instituțională și citită de doi oameni?
- ☐ Datele reprezentantului legal la registrul de stat sunt actuale?
- ☐ Certificatele expiră în următoarele trei luni?

Notă de actualitate. Portalul EVO a trecut în 2026 la versiunea EVO 2.0, care integrează modulul de împuterniciri, funcționalitățile MCabinet și notificările. Verificați la evo.gov.md, fiindcă serviciile se reorganizează des și denumirile se schimbă mai repede decât se rescriu ghidurile.

11. Revizuire și versionare

Documentul se revizuieste **semestrial**, mai des decât celelalte din kit, fiindcă serviciile publice digitale se schimbă rapid. Se revizuieste imediat când un serviciu pe care îl folosiți își schimbă denumirea sau modul de acces.

Versiunea	Data	Ce s-a schimbat	Aprobat de
1.0	[DATA]	Versiunea inițială, adoptată din Digital Civic Kit	[ORGANUL CARE APROBĂ]

Digital Civic Kit, elaborat în cadrul proiectului CivicLink Moldova, implementat de Fundația „Laboratorul de Inițiative pentru Dezvoltare” (LID Moldova) în parteneriat cu People in Need Moldova, cu finanțarea Uniunii Europene.

Drepturile asupra Digital Civic Kit aparțin LID Moldova. Organizațiile participante în proiect au dreptul de a utiliza și adapta acest document pentru uz intern, fără drept de comercializare, sublicențiere sau redistribuire către terți ca produs propriu.