DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Bune practici privind politica de gestionarea a parolelor

AUGUST 2025

TLP:CLEAR

CUPRINS

Bune practici pentru elaborarea unei politici privind parolele

1. Introducere

Identitatea digitală este deseori supusă unor amenințări din partea unei game largi de actori rău-intenționați, care vor să compromită conturi online, cu scopuri pecuniare sau non-pecuniare.

Fiecare persoană fizică trebuie să ia măsuri proprii pentru a preîntâmpina acest tip de incidente, iar orice organizație trebuie să depună eforturi concrete pentru a asigura integritatea online a membrilor săi. În acest sens, un set de măsuri foarte ușor de implementat și fără costuri este a adopta un set de reguli pentru utilizarea parolelor pentru conturi online, fie ele bancare, de social-media sau de mail.

2. Domeniu de aplicare

Documentul este parte a unui set de recomandări privind politicile de securitate propuse de Directoratul Național de Securitate Cibernetică cu scopul de a contribui la realizarea unui spațiu cibernetic sigur, respectiv pentru a veni în sprijinul instituțiilor care își desfășoară activitatea în spațiul cibernetic civil românesc.

Acest document poate să servească organizațiilor, ca un punct de pornire în elaborarea propriilor politici de gestionare a parolelor. Definirea unor politici de gestionare a parolelor, contribuie la cultivarea încrederii și protejarea resurselor digitale ale unei organizații, prin securizarea resurselor digitale a membrilor acelei organizații. Persoanele fizice pot utiliza măsurile și elementele de conduită prezentate, care pot fi adoptate pentru o mai bună protecție personală.

3. Roluri și responsabilități

Structura responsabilă cu securitatea informațiilor are atribuția de a elabora și actualiza conținutul politicii de parole, în conformitate cu bunele practici și reglementările în vigoare.

CISO validează și aprobă versiunea finală a documentului, care este ulterior transmisă conducerii pentru aprobare oficială.

După obținerea aprobării, structura responsabilă cu securitatea informațiilor are obligația de a disemina politica către toți membrii organizației, în colaborare cu departamentele implicate în instruirea și formarea angajaților.

4. Măsuri din cadrul politicii

4.1 Utilizarea parolei

4.1.1 Parola trebuie să aibă un grad adecvat de complexitate, astfel încât să reducă riscul de compromitere a acesteia la un nivel acceptabil. Astfel:

- Parolele trebuie să aibă cel puțin 14 caractere;
- Pentru angajații care gestionează date personale sau alte date sensibile, precum și pentru cei care au drepturi de administrator în rețele și sisteme informatice, parola trebuie sa aibă cel puțin 16 caractere.
- Nu trebuie acceptate parolele care conțin *user name,* numele sau prenumele utilizatorului sau alte date publice ale acestuia.
- Nu trebuie acceptate parolele care sunt cel mai des folosite pe Internet. Organizațiile ar trebui să aibă o bază de date cu aceste parole.
- O parolă complexă ar trebui să aibă cel puțin trei dintre următoarele categorii de elemente:
    - Cel puțin o literă mare;
    - Cel puțin o literă mică;

- Cel puțin un număr;
- Cel puțin un caracter special (!@#$).

4.1.2 Pentru a scădea și mai mult riscul de compromitere a unei parole, pe lângă respectarea regulilor de creare a acestora, o practică foarte bună este schimbarea periodică a parolei, respectând câteva reguli:

- În toate cazurile, parolele pre-stabilite (default) trebuie schimbate cu parole proprii, atunci când este recepționat dispozitivul/contul;
- Sistemele ar trebui să permită utilizatorilor să schimbe/reseteze parolele în orice moment;
- Intervalele de timp în care este valabilă o parolă trebuie să fie prestabilite și menționate în documentele de tip Regulament de Ordine Internă;
- Perioada maximă de reînnoire a parolei nu trebuie să depășească 12 luni;
- Interzicerea re-utilizării cel puțin a ultimelor două versiuni ale parolei;
- Regulile generale de schimbare a parolei trebuie implementate și pentru telefoanele și tabletele organizației.

Excepții:

- În situația în care codul este un element suplimentar la un identificator de acces fizic, precum un card inteligent sau un token;
- Atunci când sistemul nu este conectat la o rețea și dispune de măsuri solide de securitate fizică.

4.1.3 Reguli generale de gestionare:

- Parolele nu trebuie împărțite între mai mulți utilizatori;
- Parolele nu trebuie scrise pe format fizic lăsat la vedere;
- Parolele nu trebuie transmise prin e-mail, SMS sau convorbiri telefonice;
- În cazul folosirii unui „Password Manager”, trebuie folosite doar acele soluții de „Password Manager” autorizate de organizație;
- Nu trebuie folosită funcția „Remember password” a browserelor sau aplicațiilor;
- Orice suspiciune rezonabilă de compromitere a parolei trebuie raportată.

4.2 Autentificarea cu doi factori

Autentificarea cu doi factori (Two Factor Authentification sau 2FA) este obligatorie pentru conturile privilegiate, accesul de la distanță și aplicațiile care gestionează date sensibile.

- Utilizatorii trebuie să activeze 2FA imediat ce opțiunea este disponibilă pe platformele și sistemele organizației;
- Structura cu atribuții în gestionarea parolelor interne trebuie să asigure suport și instruire pentru configurarea corectă a 2FA.
- Codurile OTP (One-Time Password) trebuie să aibă o durată limitată de valabilitate (30–60 secunde);
- Sistemele trebuie să permită metode 2FA variate (aplicații mobile, token-uri, SMS/e-mail), în funcție de nivelul de risc;
- Dispozitivele asociate 2FA (telefoane, token-uri, smartcard-uri) trebuie protejate prin parolă/PIN și raportate imediat dacă sunt pierdute sau furate.

4.3 Autentificarea Multifactor

Autentificarea Multifactor (MFA) presupune combinarea a cel puțin doi factori de autentificare din categorii diferite:

1. Element de memorat (parolă, PIN);

2. Element fizic (token, smartcard, aplicație de autentificare);
3. Element biometric (amprentă, recunoaștere facială)

Principii pentru utilizarea MFA:

- MFA este obligatorie pentru accesul la servere, baze de date, sisteme critice și conturi cu privilegii administrative.
- Factorii utilizați trebuie să fie independenți și imposibil de compromis simultan;
- Nu este permisă validarea multiplă pe baza aceluiași tip de factor (ex.: parolă + PIN derivat din parolă);
- Configurațiile MFA trebuie aprobate de echipa de securitate IT și testate periodic pentru funcționalitate și reziliență.

4.4 Autentificare biometrică

Pe măsură ce tehnologia evoluează, metodele de autentificare nu se mai limitează doar la utilizarea parolelor clasice. Autentificarea biometrică (recunoașterea facială, amprentele digitale sau scanarea irisului) a devenit o opțiune tot mai utilizată, fie ca alternativă, fie ca măsură suplimentară de securitate (în cadrul autentificării multi-factor).

Utilizarea autentificării biometrice este permisă doar dacă sunt îndeplinite următoarele condiții:

- Echipamentul utilizat pentru autentificare este aprobat și configurat corespunzător;
- Datele biometrice sunt păstrate în siguranță, stocate local sau într-un sistem care respectă standardele de securitate și confidențialitate;

5. Instruirea privind protejarea parolelor

5.1 Responsabilități privind instruirea

- Departamentul de Securitate IT, în colaborare cu HR, are obligația de a organiza și coordona instruirile privind protejarea parolelor;
- Toți angajații, colaboratorii și terții care utilizează resursele IT ale organizației sunt obligați să participe la aceste instruiri.

5.2 Momentul instruirii

- Instruirea inițială trebuie efectuată la momentul angajării sau înainte de acordarea accesului la resursele IT;
- Reluarea instruirii se va face periodic, cel puțin o dată la 12 luni;
- Instruiri suplimentare trebuie efectuate atunci când apar modificări semnificative în politica de parole sau în infrastructura tehnică.

5.3 Conținutul instruirii

- Prezentarea regulilor de creare și utilizare a parolelor complexe;
- Exemple de practici interzise (partajarea parolelor, reutilizarea acelorași parole, stocarea în locuri nesigure);
- Demonstrarea utilizării corecte a autentificării 2FA/MFA, atunci când este aplicabilă.

5.4 Testarea și evaluarea instruirii

- După instruire, participanții trebuie să parcurgă un test de verificare a cunoștințelor;
- Testarea practică a parolelor se va face prin simulări controlate (ex.: audituri interne de securitate, testare parole împotriva bazelor de date cu parole comune);
- Rezultatele testelor vor fi analizate de echipa de securitate IT, iar deficiențele constatate vor fi remediate prin instruiri suplimentare individuale sau de grup.

5.5 Evidență și conformitate

- Departamentul de resurse umane va păstra evidența tuturor angajaților care au parcurs instruirile și testările;
- Lipsa participării la instruiri sau rezultate slabe la testări pot atrage măsuri administrative conform regulamentului intern;
- Departamentul IT/security raportează anual managementului gradul de conformitate privind instruirea și protecția parolelor.

6. Încălcarea prevederilor politicii

Nerespectarea politicii privind parolele este considerată un risc major de securitate și va atrage consecințe corespunzătoare. În situațiile în care se constată abateri deliberate sau repetate de la prezenta politică, organizația poate aplica măsuri disciplinare progresive, în conformitate cu legislația și regulamentele interne, inclusiv:

- avertisment scris;
- suspendarea temporară a accesului la resursele IT;
- restricționarea unor privilegii de acces;
- încetarea contractului de muncă sau de colaborare, în cazuri grave de nerespectare.

De asemenea, orice incident generat de încălcarea acestei politici va fi raportat către structura responsabilă pentru analizat și documentat pentru a preveni reapariția situațiilor similare.

7. Practici utile în gestionarea parolelor

Distribuirea prin e-mail a parolelor

Deși e-mailul nu este cel mai sigur mediu în toate cazurile, poate fi folosit atunci când:

- Nu este utilizat un sistem extern de e-mail.
- E-mailul este trimis criptat (cum ar fi Office 365)
- Combinația specificată de nume de utilizator și parolă expiră după prima utilizare sau, dacă nu este utilizată, după o anumită perioadă.

Password manager[1]

Un manager de parole este o aplicație care stochează și gestionează în siguranță parolele, utilizând criptarea. Un manager de parole permite:

- Generarea de parole unice și puternice;
- Memorarea și completarea automata a datelor de autentificare;
- Alertarea utilizatorului dacă parola sa a fost compromisă.

Passphrases

O practică utilizată de tot mai multe organizații este înlocuirea parolei în înțelesul ei tradițional cu așa-numitele „passphrases”. Scopul acestei practici este de a crea parole mai lungi și facilita memorarea ei de către utilizator.

Principii pentru crearea de passphrase:

[1] https://www.linkedin.com/posts/dnsc-ro_dnsc-cyber-hygene-activity-7301179390497808384-WEG9?utm_source=share&utm_medium=member_desktop&rcm=ACoAABIyjNkBSeTH83GpAoyJmR-nsUvsXkRw6CA accesat 14.04.2024

- Include cel puțin trei cuvinte;
- Include un element unic pentru utilizator: o poreclă, numele mamei, o cifră norocoasă etc;
- Include spații inserate aleatoriu, sporind enorm complexitatea;
- Include și litere mici și litere mari, dar în mod aleatoriu;
- Poate include greșeli gramaticale sau regionalisme.

Exemple:

☒ filmedeactiune2003

☒ Filme de Actiune! 2003

8. Termeni și definiții

Termen	Definiție
Blacklist	Listă care conține și blochează accesul utilizatorilor sau entităților cu risc ridicat[2].
Brute Force Attack	Metodă automatizată de ghicire a parolelor prin testarea tuturor combinațiilor posibile[3].
CISO	membru al conducerii responsabil pentru securitatea informațiilor și a sistemelor informatice ale unei organizații, inclusiv securitatea cibernetică, dezvoltarea politicilor de securitate și protejarea datelor critice împotriva amenințărilor cibernetice.
Date biometrice	Date cu caracter personal care rezultă în urma unor tehnici de prelucrare specifice referitoare la caracteristicile fizice, fiziologice sau comportamentale ale unei persoane fizice care permit sau confirmă identificarea unică a respectivei persoane, cum ar fi imaginile faciale sau datele dactiloscopice[4].
Multi-Factor Authentication (MFA)	Proces de autentificare care necesită cel puțin doi factori diferiți de verificare[5].
Passphrase	Spre deosebire de parolele obișnuite, care pot fi combinații aleatoare de litere și cifre, o passphrase se bazează pe memorabilitatea unei fraze mai lungi, oferind astfel un nivel de securitate mai ridicat datorită complexității și lungimii sale.
Password Manager	Aplicație care stochează și generează parole securizate[6].

[2] https://www.twingate.com/blog/glossary/blacklist accesat 13.04.2025.
[3] https://www.linkedin.com/posts/dnsc-ro_dnsc-cyber-awareness-activity-7297163085172109313-qxAm?utm_source=share&utm_medium=member_desktop&rcm=ACoAABIyjNkBSeTH83GpAoyJmR-nsUvsXkRw6CA accesat 13.04.2025.
[4] https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:32016R0679 accesat 14.04.2025
[5] https://support.microsoft.com/en-us/topic/what-is-multifactor-authentication-e5e39437-121c-be60-d123-eda06bddf661 accesat 13.04.2025.
[6] https://www.cmu.edu/iso/governance/guidance/password-managers.html accesat 13.04.2025.

Token	Componentă a unui dispozitiv de securitate cu autentificare care poate fi utilizat pentru a autoriza utilizarea serviciilor informatice[7].

Tabel 2. Termeni și definiții

Autori: Vlad Drăguș, Simona Tărăbășanu- Mihăilă, Ioana Murărașu

TLP:CLEAR se poate folosi atunci când informațiile prezintă un risc minim de utilizare abuzivă, în conformitate cu normele și procedurile aplicabile pentru publicare. Sub rezerva regulilor standard ale drepturilor de autor, infor mațiile TLP:CLEAR pot fi partajate fără restricții.

https://www.dnsc.ro/

[7] https://www.techtarget.com/searchsecurity/definition/security-token accesat 13.04.2025.

ANEXA – Model pentru Politica privind parolele

1. Introducere

Această politică stabilește reguli și bune practici privind stabilirea parolelor de către angajați, colaboratori și reprezentanți ai [Numele Organizației], pentru a proteja integritatea și confidențialitatea datelor organizației și a membrilor săi.

2. Domeniu de aplicare

Politica se aplică tuturor persoanelor care lucrează în cadrul [Numele Organizației], indiferent de tipul contractului sau de poziția ocupată, atunci când:

- Încep raportul de muncă cu organizația;
- Creează noi conturi legate direct de activitatea din cadrul organizației;
- Primesc și configurează dispozitive de la locul de muncă;

3. Scop

Această politică:

- Stabilește cerințele și standardele minime pentru crearea, utilizarea și gestionarea parolelor asociate sistemelor, aplicațiilor și resurselor IT ale [Numele Organizației];
- Stabilește măsuri pentru protejarea parolelor împotriva divulgării, reutilizării necorespunzătoare sau compromiterii;
- Previne crearea și utilizarea conturilor cu parole slabe, nesigure sau neconforme cu cerințele organizației.
- Stabilește cadrul pentru instruirea personalului cu privire la politica de parole.

4. Roluri și responsabilități

[Structura/Departamentul responsabil cu securitatea informațiilor] are atribuția de a elabora și actualiza conținutul acestei politici de parole, în conformitate cu bunele practici și reglementările aplicabile.

[CISO / Funcția echivalentă] validează și aprobă versiunea finală a documentului, care este ulterior supusă aprobării de către [Conducerea organizației].

După obținerea aprobării, [Structura/Departamentul responsabil cu securitatea informațiilor] are obligația de a disemina politica către toți membrii organizației, în colaborare cu [Departamentul HR / Structura cu atribuții în instruirea și formarea angajaților].

5. Măsuri privind gestionarea parolelor

- Complexitatea parolei

Parolele pentru conturile de serviciu ale angajaților trebuie să conțină cel puțin [14] caractere.

Fiecare parolă va conține cel puțin o literă mare, o cifră și un simbol -@#$%.

Pentru angajații care gestionează date personale sau alte date sensibile [HR,Economic, DPO] , precum și pentru cei care au drepturi de administrator în rețele și sisteme informatice, parola trebuie sa aibă cel puțin [16] caractere.

- Reguli de schimbare a parolei

Parolele aferente conturilor angajaților vor fi valabile maxim [6 luni]. Pentru noua parolă, este interzisă reutilizarea celei anterioare, respectiv a ultimelor [două] versiuni utilizate.

- Autentificare cu doi factori (2FA)

Pentru conturile critice, accesul de la distanță și conturile cu privilegii extinse din cadrul [Numele Organizației], autentificarea se va realiza obligatoriu cu doi factori (parolă + un cod unic generat sau transmis printr-un canal securizat).

Factorul secundar de autentificare poate fi reprezentat de [o aplicație de autentificare, token hardware, SMS sau e-mail securizat], infrastructura pusă la dispoziție de [Departamentul responsabil].

Aplicația utilizată pentru autentificarea cu doi factori va fi [Numele aplicației și furnizorul]

Utilizatorii au obligația de a păstra în siguranță dispozitivele asociate autentificării [telefon, token, smartcard] și de a raporta imediat pierderea sau compromiterea acestora către [Departamentul responsabil].

Codurile generate prin 2FA vor avea o perioadă limitată de valabilitate și nu trebuie comunicate altor persoane.

- Autentificare multifactor (MFA)

Pentru accesul la servere, aplicații critice și conturi administrative ale [Numele Organizației], autentificarea se va realiza obligatoriu printr-un mecanism multifactor (MFA), utilizând cel puțin doi factori din categorii diferite:

1. Element de memorat (parolă, PIN);
2. Element fizic (token, smartcard, aplicație de autentificare);
3. Element biometric (amprentă, recunoaștere facială)

Factorii utilizați trebuie să fie independenți și imposibil de compromis simultan.

Este interzisă validarea multiplă prin factori de același tip (ex.: parolă + PIN derivat din parolă).

Configurațiile MFA vor fi stabilite și verificate periodic de către [Departamentul responsabil cu securitatea IT], care are obligația să testeze funcționalitatea și reziliența acestora împotriva atacurilor cibernetice.

- Autentificarea biometrică

Autentificarea biometrică (ex.: amprentă, recunoaștere facială, recunoaștere vocală) poate fi utilizată pentru accesul la dispozitive și sisteme informatice ale [Numele Organizației], atunci când infrastructura tehnică o permite și există un nivel adecvat de securitate.

Implementarea soluțiilor de autentificare biometrică se va realiza numai cu aprobarea [Responsabilului cu protecția datelor cu caracter personal] și în conformitate cu Regulamentul (UE) 2016/679 (GDPR) și cu legislația națională aplicabilă.

Datele biometrice vor fi prelucrate exclusiv în scopul autentificării și nu vor fi utilizate pentru alte scopuri. Acestea trebuie stocate în formă criptată și protejate împotriva accesului neautorizat.

Utilizatorii vor fi informați cu privire la modalitatea de colectare, utilizare și stocare a datelor biometrice, precum și la drepturile lor legale.

În caz de nefuncționare a mecanismului biometric, [Departamentul responsabil] trebuie să asigure metode alternative de autentificare (ex.: MFA sau 2FA), pentru a nu afecta continuitatea activității.

Orice incident de securitate legat de datele biometrice trebuie raportat imediat către [Responsabilul cu securitatea informațiilor] și către [Responsabilul cu protecția datelor cu caracter personal].

- Alte reguli

- Angajații nu vor divulga altor persoane parola stabilită pentru conturile și dispozitivele proprii;

- Angajaților le este interzis a lăsa la vedere înscrisuri fizice reprezentând parolele stabilite pentru dispozitivele și conturile proprii.

4. Instruirea privind politica de parole

[Departamentul responsabil cu securitatea informațiilor], în colaborare cu [Departamentul HR / de instruire], va organiza sesiuni de instruire pentru toți angajații, colaboratorii și terții care utilizează resursele IT ale [Numele Organizației].

Instruirea se realizează:

- la angajarea persoanei sau înainte de acordarea accesului la resurse IT;

- periodic, cel puțin o dată la [12 luni];

- suplimentar, ori de câte ori apar modificări semnificative în politica de parole sau în infrastructura IT.

Sesiunile de instruire vor include: regulile de creare și utilizare a parolelor complexe, utilizarea corectă a mecanismelor 2FA/MFA, măsuri de protecție a dispozitivelor și raportarea incidentelor.

După instruire, participanții vor fi supuși unor teste de verificare a cunoștințelor și unor verificări practice prin simulări controlate (ex.: testarea parolelor împotriva listelor cu parole comune).

Rezultatele testărilor vor fi analizate de [Departamentul responsabil cu securitatea IT], iar persoanele care nu respectă cerințele vor parcurge instruiri suplimentare.

[Departamentul HR] va păstra evidența instruirilor și a rezultatelor testelor, iar gradul de conformitate va fi raportat anual către [Conducerea organizației].

5. Încălcarea prevederilor politicii

Nerespectarea acestei politici poate duce la măsuri disciplinare, care pot include avertisment, suspendare a accesului la resursele IT sau încetarea contractului de muncă, în conformitate cu legislația și regulamentele interne.

6. Contact

Dacă angajații au întrebări despre această Politică, aceștia trebuie să contacteze [persoana de contact].

N.B – Toate elementele indicate între parantezele drepte [ ] trebuie înlocuite cu denumirile, titlurile, departamentele sau aplicațiile specifice organizației, astfel încât politica să reflecte configurarea și structura internă reală, respectiv opțiunile proprii privind rigorile aplicabile de la caz la caz.