

Ghidul de utilizare a rețelelor sociale în sectorul public



Cuprins

I. Reglementare.....	1
II. Scop.....	1
III. Introducere.....	1
IV. Gestionarea contului.....	3
Deschiderea contului.....	3
Identificarea contului.....	3
Menținerea contului.....	3
V. Procesul de creare a contului.....	4
Roluri și responsabilități.....	4
Ghid privind conținutul.....	4
VI. Procesele de implicare a cetățenilor.....	5
Roluri și responsabilități.....	5
Norme privind conținutul.....	5
Procedee de încorporare a feedback-ului din partea cetățenilor.....	6
VII. Utilizarea de către angajat.....	6
Accesul angajatului.....	8
Conduita angajatului.....	7
VIII. Aspecte privind securitatea.....	9
IX. Aspecte de ordin legal.....	10
X. Mulțumiri.....	11

I. Cadru general

Ghidul de utilizare a rețelelor sociale în sectorul public vine să ofere informații detaliate despre tehnicile de antrenare a platformelor de socializare în activitatea cotidiană a instituțiilor publice. Documentul este un îndrumar pentru funcționarii publici și comunicatorii instituțiilor publice în vederea utilizării mijloacelor de socializare. Direcțiile specifice incluse în ghid indică cum trebuie selectate instrumentele de socializare, cum se creează conținutul pentru angajați și cetățeni, la fel oferă sfaturi privind încorporarea feedback-ului de la cetățeni, aplicarea tacticilor de implicare a cetățenilor și crearea unei strategii de social media.

Ghidul de utilizare a rețelelor sociale în sectorul public este **un material de suport** pentru ministere și departamente, realizat în scopul creării unor proceduri interne de gestionare a utilizării mijloacelor de socializare. Acesta cuprinde următoarele elemente: introducerea, gestionarea conținutului, crearea conținutului, implicarea cetățenilor, utilizarea de către angajați, aspecte privind securitatea, aspecte de ordin legal.

II. Scop

Ghidul dat este aplicabil în toate structurile guvernamentale la nivel central, inclusiv agenții și departamente. De asemenea, acesta se răsfrânge asupra părților contractate, antrenate în utilizarea mijloacelor de socializare în numele Guvernului Republicii Moldova, constituind o parte a responsabilităților contractuale. Principiile de direcționare vor fi neutre în raport cu instrumentele utilizate și vor avea un caracter general aplicabil tuturor mijloacelor de socializare. Ținând cont de natura dinamică a mijloacelor de socializare, ghidul va fi revizuit și modificat la necesitate. De asemenea, documentul va considera canalele de comunicare din cadrul platformelor de socializare drept canale oficiale de comunicare într-o unitate guvernamentală.

III. Introducere

Tehnologia informației evoluează constant, punând la dispoziție noi oportunități de transformare a instituțiilor de stat și noi forme de comunicare cu publicul. Instrumentele de comunicare oferite de mijloacele de socializare fac parte din șirul de tehnologii moderne care înlesnesc schimbul interactiv de informații, interoperabilitatea, precum și colaborarea în rândul angajaților instituțiilor de stat și între aceștia și publicul larg.

Peste 250 de mii de cetățeni moldoveni sunt momentan pe Facebook. Numărul

"Mijloacele de socializare" și "Web 2.0" sunt termeni generici și cuprind diverse activități, ce integrează tehnologii, interacțiune socială și crearea conținutului. Mijloacele de socializare preiau diverse forme, cum ar fi blogurile, wikis (pagini de grup redactate de utilizatori), schimb de fișiere foto și video, podcasts (distribuire de fișiere multimedia), socializare pe net, aplicații tip mash-up și spații virtuale. Mijloacele de socializare reprezintă un set de tehnologii online, pagini, și practici folosite pentru a face schimb de opinii și experiență prin antrenarea utilizatorilor.

utilizatorilor de Odnoklassniki și v Kontakte este de 2 ori mai mare. Pe cele două rețele rusești sunt în total 460 de mii de moldoveni.

Facebook-ul este accesat mai mult de femei -147 mii sau 55,4%. Numărul bărbaților este de 117 mii, sau 44,6%.

Moldovenii sunt tot mai mobili. Astfel, 1 din 5 utilizatori accesează Facebook-ul de pe telefonul mobil sau de pe tablete mobile.

Prezența pe mijloacele de socializare a unei instituții de stat a devenit o reflecție a unui proces de comunicare activ și transparent. Activitățile de socializare contribuie la îmbunătățirea interactivității dintre o unitate guvernamentală și publicul pe care aceasta o deservește, oferind noi oportunități de a accesa segmente de populație care nu utilizează mijloace media tradiționale. Beneficiul de pe urma utilizării mijloacelor de socializare de către instituțiile de stat poate fi unul major, în cazul în care există o strategie de socializare bine gândită. Instituția guvernamentală va realiza o mai bună transparență a activităților, o relație interactivă cu cetățenii, o mai mare asumare a responsabilităților pentru politicile și serviciile guvernamentale, astfel căpătând mai multă încredere în rândul populației. Instituțiile publice sunt încurajate să utilizeze tehnologiile de socializare pentru a-și îmbunătăți comunicarea, colaborarea și schimbul de informații cu publicul larg, cu alte structuri de stat, cu sectorul privat, cu reprezentanții comunității internaționale, precum și cu cetățenii aflați peste hotare.

Instrumentele de comunicare utilizate de instituțiile publice, inclusiv mijloacele de socializare, trebuie să țină cont de obiectivele de comunicare, colaborare și schimbul de informații. Totuși, utilizarea mijloacelor de socializare va ține cont și de aspectele de securitate, confidențialitate și profesionalism.

Prezentul document este elaborat pentru a informa angajații și pentru a asigura consecvența utilizării mijloacelor de socializare în cadrul tuturor instituțiilor publice. Fiecare structură guvernamentală va perfectă modificările necesare la acest document în funcție de contextul de serviciu, concomitent oferindu-le angajaților sprijin și ghidare pentru o utilizare inteligentă și productivă a instrumentelor de socializare.

Ghidul a fost realizat cu sprijinul "The Research Foundation of State University of New York" și suportul financiar din partea Ambasadei SUA în Republica Moldova.

Documentul a fost consultat cu reprezentanții societății civile și comunicatorii Guvernului și este recomandat APC-urilor.

IV. Gestionarea contului

Conturile instituțiilor publice pe rețele de socializare sunt considerate drept canale oficiale de comunicare ale acestora. Deoarece nu există mari dificultăți de ordin tehnic în procesul de creare a unui cont, ulterior pot apărea probleme legate de menținerea integrității conținuturilor. Astfel, fiecare unitate va avea în vedere proceduri de securitate la crearea contului, identificarea contului și menținerea informațiilor de pe acesta.

Crearea contului

Fiecare unitate de stat va elabora o procedură de autorizare pentru funcționarii abilitați să deschidă cont de serviciu. În cooperare cu departamentul tehnologii informaționale al instituțiilor, șeful departamentului comunicare sau un reprezentant al acestui departament vor fi instanțele care vor autoriza și revizui decizia de deschidere a contului. În acest sens, sarcinile șefului departamentului comunicare vor include evaluarea tuturor cererilor de utilizare a mijloacelor de socializare, verificarea angajaților cu acces autorizat la instrumentele de socializare și consultarea cu departamentul tehnologii informaționale pentru a preveni riscurile ce pot apărea odată cu accesarea platformelor de socializare.

Identificarea contului

Orice cont de socializare al unei unități guvernamentale va indica clar că acesta este gestionat de unitatea respectivă. Orice cont de socializare gestionat de o unitate de stat va afișa la un loc vizibil informațiile de contact care să cuprindă cel puțin:

- Numele persoanelor responsabile de gestionarea contului
- Funcția acestora
- Contacte

Gestionarea contului

Conducerea instituțiilor publice va desemna responsabili de gestionarea conturilor pe rețelele de socializare și administratori de conturi. Fiecare cont oficial va avea un log separat corespunzător fiecărei parole, deoarece utilizarea aceleiași parole pentru accesarea mai multor conturi crește vulnerabilitatea acestor conturi. În cazul în care un administrator de cont pe rețelele sociale va fi înlăturat de la administrarea contului sau destituit din funcție, partea responsabilă de gestionarea conturilor va modifica imediat parola și informațiile de pe cont în scopul menținerii controlului asupra contului deschis în cadrul instituției. Informațiile noi și modificările efectuate la cont vor fi puse la dispoziția părții responsabile imediat după producerea schimbării.

În scopul evitării situațiilor de risc care pot afecta imaginea instituției, partea responsabilă de gestionarea conturilor va întreprinde măsurile necesare pentru a asigura securitatea contului.

V. Procesul de creare a conținutului

Conținutul de pe conturile de socializare plasat în numele instituției de stat și distribuit prin canalele oficiale de socializare va fi considerat drept informație cu caracter oficial. Ținând cont de aceasta, se impune asigurarea corectitudinii conținutului pentru a păstra integritatea datelor. Mai mult, limbajul utilizat pe cont va corespunde întocmai limbajului comunicărilor oficiale. Prin urmare, unitățile din cadrul instituțiilor de stat vor desemna părți responsabile de crearea și aprobarea informațiilor plasate pe conturile de socializare bazându-se pe setul minim de cerințe enumerate mai jos.

Roluri și responsabilități

Fiecare instituției publice trebuie să elaboreze o procedură de autorizare a angajaților cu drept de contribuție la conținut. Persoanele cărora li s-au desemnat aceste roluri vor fi responsabile de actualizarea la timp a conținutului plasat pe contul oficial. Fiecare unitate guvernamentală își va elabora o procedură adecvată contextului de serviciu și va respecta cel puțin următoarele principii:

- Doar funcționarii autorizați vor avea dreptul să plaseze informații pe paginile oficiale de socializare, Web 2.0 și alte rețele de socializare din numele instituției de stat. Acest principiu se va aplica în toate cazurile, fie că pagina este gestionată din interiorul instituției fie din exterior.
- Angajații instituțiilor de stat nu-și vor exprima opiniile din numele instituției pe care o reprezintă pe forumurile neguvernamentale; excepție vor fi cazurile când plasarea acestor opinii este autorizată de persoana responsabilă de comunicarea pe rețelele de socializare oficiale, de obicei șeful departamentului comunicare.
- Atunci când postează sau fac schimb de informații pe forumurile externe de socializare, angajații instituțiilor de stat autorizați să comunice din numele instituției se vor legitima indicând: 1) numele deplin; 2) funcția; 3) direcția în care activează și 4) datele de contact. Postările se vor limita doar la scopul prevăzut de autorizare pentru fiecare caz specific.

Conținutul

Angajații instituțiilor guvernamentale care folosesc mijloacele de socializare pentru a se exprima din numele instituției de stat trebuie să țină cont că afirmațiile sunt făcute din numele instituției. De aceea, aceștia vor face postări sau comentarii echilibrate. Informațiile de pe paginile guvernamentale care vor conține oricare dintre însușirile enumerate mai jos nu vor fi postate:

- Limbaj sau conținut vulgar;
- Limbaj sau tonalitate ofensive;
- Conținut care promovează, încurajează sau perpetuează discriminarea pe criterii de rasă, convingeri, culoare, vârstă, religie, statut matrimonial, naționalitate, dezabilitate fizică sau mintală sau orientare sexuală;
- Conținut obscen sau link-uri la conținut obscen;
- Solicitări de afaceri;
- Desfășurarea sau încurajarea activităților ilegale;
- Informații care ar putea pune în pericol siguranța sau securitatea publică sau securitatea sistemelor publice;
- Conținut care încalcă interesele de proprietate juridică a oricărei alte părți;
- Promovarea sau opunerea față de vreun candidat la funcție politică sau promovarea sau opunerea față de orice plebiscit;
- Utilizatorii nu vor posta sau dezvălui informații ce țin de drepturile de proprietate, date cu caracter confidențial, informații secrete, date personale sau date ce țin de proprietatea intelectuală a Guvernului.

VI. Implicarea cetățenilor

Informațiile care se conțin pe conturile de socializare ale instituțiilor de stat pot veni și de la publicul larg. Dat fiind caracterul public al rețelelor de socializare și speranța la o participare activă din partea cetățenilor, va fi necesar ca instituțiile de stat să-și elaboreze procedee eficiente pentru gestionarea implicării cetățenilor, inclusiv desemnarea clară de roluri și responsabilități, norme cu privire la informațiile postate de cetățeni și proceduri de încorporare a feedback-ului din partea acestora.

Roluri și responsabilități

Toate informațiile din partea publicului vor fi arbitrate de angajați autorizați ai instituției guvernamentale, aceștia fiind instruiți să monitorizeze și să răspundă la comentariile și conținutul plasate de cetățeni pe rețelele de socializare. Fiecare unitate guvernamentală va desemna o asemenea persoană (sau mai multe) în funcție de contextul de serviciu. Rolurile și responsabilitățile acestor angajați vor stipula și intervalul de timp acceptabil pentru a primi postări și pentru a răspunde la comentarii și solicitări.

Norme privind conținutul din partea cetățenilor

Unul dintre cele mai importante obiective pe care instituțiile de stat doresc să-l realizeze prin intermediul rețelelor de socializare este interacțiunea efectivă cu cetățenii în condiții de risc minim. Pentru aceasta, instituțiile de stat sunt încurajate să-și elaboreze un cod public de conduită pentru utilizatorii publici, cu descrierea comportamentului adecvat din partea cetățenilor utilizatorilor. Codul trebuie să fie comunicat explicit pe fiecare

rețea de socializare. De asemenea, codul public de conduită va indica clar tipurile de conținut interzis și modul în care va fi tratat asemenea conținut. Codul va aborda cel puțin următoarele aspecte:

- Comentariile irelevante sau ieșite din context.
- Limbajul vulgar.
- Comentariile care promovează discriminarea.
- Comentariile care promovează activitățile ilegale.
- Comentariile care încalcă orice drepturi legale sau drepturi asupra proprietății intelectuale.

Normele ce țin de conținut vor include și perioadele de timp alocate pentru a revizui comentariile, postările și răspunsul instituției, pentru a corespunde așteptărilor publicului.

Angajații responsabili de monitorizarea și plasarea răspunsurilor vor fi instruiți corespunzător cu privire la metodele de aplicare a normelor de reglementare a conținutului. Cenzurarea neadecvată a postărilor va restrânge colaborarea și participarea publicului. Angajații responsabili de monitorizare vor face tot posibilul pentru a include orice feedback semnificativ din partea cetățenilor, fie acesta pozitiv sau negativ.

Procedee de încorporare a feedback-ului din partea cetățenilor

Acțiunile de socializare create cu scopul de a antrena publicul în deciziile luate de instituțiile de stat în materie de ghid, ordonanțe și servicii sau orice alte acțiuni ale Guvernului vor fi bazate pe un șir de procedee, care vor articula modul de încorporare a feedback-ului. Partea responsabilă de monitorizare și răspuns la feedback-ul publicului va stabili o procedură clară de comunicare cu alte direcții din cadrul instituției de stat, astfel asigurând utilizarea adecvată a feedback-ului solicitat prin rețelele de socializare. Procedura selectată va fi explicată clar și afișată pe canalul de socializare utilizat de instituție.

VII. Utilizarea contului de către angajați

Utilizarea rețelelor de socializare în cadrul unei instituții guvernamentale poate fi grupată în 3 categorii: utilizarea de către întreaga instituție – în acest caz angajații folosesc canalul de socializare din numele instituției; utilizarea profesională – angajații instituției folosesc mijloacele de socializare în scopul dezvoltării profesionale și utilizarea personală – angajații accesează instrumentele de socializare în timpul orelor de lucru în scopuri personale. Fiecare unitate guvernamentală va decide dacă permite utilizarea

mijloacelor de socializare de către angajați și va stabili limitele adecvate de utilizare. Managerii din cadrul instituției vor fi responsabili să comunice regulile de utilizare și să asigure respectarea acestora de către angajați. Fiecare instituție de stat va aborda cel puțin trei aspecte legate de utilizarea de către angajați: accesul angajaților, utilizarea admisibilă și comportamentul angajaților.

Accesul angajaților

- Fiecare instituție de stat va stabili în ce măsură va permite angajaților accesul la instrumentele de socializare. Accesul poate fi îngăduit tuturor angajaților, poate fi limitat în dependență de funcția deținută sau poate fi permis doar accesul la un număr prestabilit de rețele. Fiecare unitate guvernamentală va determina tactica de utilizare în funcție de contextul de serviciu.

Dacă accesarea este permisă doar unui grup de angajați sau pe un număr limitat de rețelele de socializare, instituția de stat va elabora și afișa următoarele proceduri:

- Va fi stabilită o procedură prin care angajații vor solicita accesul la instrumentele de socializare. Această procedură va detalia următoarele:
 - a) pașii pe care trebuie să-i întreprindă un angajat atunci când solicită acces;
 - b) materialele care trebuie prezentate pentru a-i sprijini solicitarea;
 - c) decizia persoanei autorizate cu privire la solicitare;
 - d) temeiurile pe care se va baza decizia;
 - e) în ce mod și în cât timp va fi comunicată decizia solicitantului.
- Va fi stabilită o procedură prin care angajații solicită utilizarea unor rețele de socializare specifice. Această procedură va detalia următoarele:
 - a) materialele care trebuie prezentate pentru a sprijini solicitarea de acces a rețelei;
 - b) persoana autorizată să decidă asupra solicitării;
 - c) temeiurile pe care se va baza decizia;
 - d) în ce mod și în cât timp va fi comunicată decizia solicitantului.

În general, principalul criteriu de aprobare a accesului angajaților trebuie să fie îmbunătățirea performanței lor profesionale care să ducă la sporirea randamentului și rezultatelor produse.

Utilizarea admisibilă

Regulile de utilizare a rețelelor de socializare de către angajați sunt similare cu acelea care reglementează accesul la internet, email și alte TI. Unitățile guvernamentale sunt încurajate să verifice mai întâi dacă pot aplica ghidurile existente și, la necesitate, să efectueze modificările de rigoare pentru a le ajusta la mijloacele de socializare.

În timpul orelor de lucru sau atunci când folosesc un dispozitiv din inventarul instituției de stat, angajații nu vor avea dreptul să utilizeze rețelele de socializare în scopuri politice, pentru a realiza tranzacții comerciale sau afaceri personale. Angajații trebuie să țină cont că utilizarea necorespunzătoare a mijloacelor de socializare poate servi drept temei pentru acțiuni disciplinare. Normele de utilizare admisibilă trebuie să cuprindă următoarele arii:

- **Utilizarea din numele instituției.** Angajații responsabili de menținerea prezenței instituției pe rețelele de socializare au dreptul să le utilizeze în beneficiul instituției. Acest lucru presupune monitorizarea forumurilor sociale relevante, menținerea prezenței instituției pe rețelele de socializare și monitorizarea tendințelor și a practicilor optime de utilizare a rețelelor de socializare în instituțiile de stat. Scopurile utilizării rețelelor de socializare sunt următoarele:
 - Interacțiunea cu cetățenii în timp real;
 - Informarea cetățenilor;
 - Consultarea inițiativelor și documentelor publice;
 - Implicarea cetățenilor în procesul de luare a deciziilor;
 - Efectuarea sondajelor de opinie.
- **Utilizarea contului în scopuri profesionale.** Personalul care accesează rețelele de socializare în vederea îmbunătățirii performanței profesionale va automonitoriza utilizarea pentru a se asigura că activitățile de pe canalele de socializare contribuie la creșterea profesională și nu o împiedică. Abilitățile căpătate de un angajat în urma utilizării rețelelor de socializare în timpul orelor de lucru trebuie să fie direct legate de sarcinile și atribuții prevăzute de fișa de post.
- **Utilizarea contului în scopuri personale.** Angajații care administrează conturile oficiale ale instituțiilor pe rețele de socializare nu vor publica opinii personale pe aceste pagini de pe contul instituției. Angajații instituțiilor publice nu pot utiliza conturile personale în timpul orelor de lucru dacă nu sunt autorizați pentru aceasta. Angajații nu vor avea dreptul să utilizeze adresa de mail sau parola de la locul de muncă pentru conturile lor personale de pe rețelele de socializare.

Comportamentul angajaților

Comportamentul angajaților pe rețelele de socializare în timpul orelor de lucru va fi reglementat de normele existente privind conduita la locul de muncă. Angajații vor manifesta precauție cu privire la informațiile lor personale sau profesionale afișate pe rețelele de socializare. Toți angajații, indiferent de gradul de acces la mijloacele de socializare, vor respecta următoarele reguli generale:

- Angajații care accesează rețele de socializare prin intermediul conturilor deschise de instituția de stat și care se exprimă din numele instituției, vor respecta toate normele ce țin de comportamentul inadmisibil la locul de muncă, inclusiv ghidurile privind comportamentul admisibil, acordurile de utilizare, prevederile referitoare la hărțuirea sexuală, etc. Toate informațiile comunicate prin rețelele guvernamentale vor avea caracter profesional și vor respecta ghidurile, normele și așteptările instituției cu privire la comunicare.
- Angajații instituției de stat vor putea să-și includă funcția oficială pe conturile personale de pe rețelele de socializare. În același timp, funcționarii care nu sunt autorizați să se exprime din numele instituției vor menționa clar că toate activitățile și comentariile de pe rețelele de socializare nu reprezintă în niciun fel poziția oficială a instituției. Termenii de utilizare vor fi clar afișați pe fiecare pagină de socializare.
- Angajatul instituției de stat va răspunde de acțiunile sale pe rețelele de socializare asigurând că acestea nu cauzează niciun prejudiciu imaginii instituției.

VIII. Aspecte privind securitatea

Rețelele de socializare prezintă riscuri de securitate. De aceea, unitățile guvernamentale vor întreprinde toate măsurile posibile pentru a-și proteja canalele de comunicare, infrastructura și informațiile private și confidențiale despre angajați și public. Cele mai frecvente modalități de a ataca securitatea rețelelor sociale includ phishing-ul datelor de autentificare, tehnici de manipulare – social engineering, falsificarea identității – spoofing și atacarea aplicației web. În același timp, pașii accelerați cu care se dezvoltă tehnologiile informaționale impun necesitatea actualizării continue a protocoalelor de securitate pentru a face față noilor amenințări de securitate. Prin urmare, fiecare unitate guvernamentala își va educa angajații privind riscurile asociate utilizării rețelelor sociale și modalităților de atenuare a acestora. În general, utilizarea paginilor de socializare va fi reglementată de normele de securitate curente, aplicate la întregul sistem de tehnologii informaționale. Pe lângă ghidul privind securitatea informațională, instituția va mai întreprinde următorii pași:

- Angajaților nu li se va fi permite să utilizeze adresa de email sau parola de la locul de muncă pentru a-și accesa conturile în rețele de socializare.
- Angajații nu vor avea "privilegii de administrator" pe calculatoarele de serviciu cu acces la internet.
- Direcția tehnologii informaționale din fiecare unitate de stat va revizui tehnologiile selectate, clienții și plug-ins-urile cu scopul de a preveni vulnerabilitatea sistemelor informatice înainte de utilizarea acestora.
- Pentru a menține securitatea utilizatorilor și a parolelor în rețeaua instituției, persoanele autorizate cu acces la rețele de socializare vor folosi nume de utilizatori și parole diferite de cele aplicate în rețeaua de serviciu.
- Se interzice transferul de date sensibile pe platformele de socializare.
- Aceste tehnologii sporesc vulnerabilitatea unui calculator la atacurile de tip *denial of service* (DoS). Utilizatorii autorizați își vor configura mijloacele de socializare, Web 2.0 sau clienții din rețelele sociale, blocând mesajele de la surse neautorizate.
- Angajații trebuie să știe ce date pot sau nu pot fi diseminate.
- Utilizatorii din cadrul unității guvernamentale vor fi instruiți în materie de securitate informatică și anume în sfera riscurilor generate de divulgarea datelor pe rețelele de socializare și mecanismelor de atacare a securității.
- Utilizatorii din cadrul instituțiilor guvernamentale vor fi instruiți cu privire la ghidurile de utilizare și securizare a mijloacelor de socializare, fapt care îi va ajuta să-și controleze mai bine propria securitate și să se protejeze mai eficient contra dezvăluirilor neatențe de informații de serviciu sensibile.
- Înainte de a autoriza accesul pe paginile de socializare, utilizatorii din cadrul instituțiilor guvernamentale vor fi instruiți cu privire la amenințările specifice asociate rețelelor sociale.

IX. Aspecte de ordin legal

Accesul la paginile de socializare și utilizarea lor în cadrul unităților de stat vor fi reglementate prin legi, ghiduri și proceduri existente și aplicabile, inclusiv **acelea** privind securitatea informațională. Toate tipurile de utilizare vor respecta aceste reguli precum și normele prevăzute de acest document. Utilizarea mijloacelor de socializare în cadrul unei instituții guvernamentale poate duce la apariția unui șir de probleme de ordin legal. Majoritatea acestora sunt evitate prin exercitarea de bun simț și respectarea normelor existente de conduită. În același timp, este important să se clarifice parametrii juridico-legali în care operează instituția, mai ales ținând cont că dezvoltarea accelerată și dinamica de dezvoltare a mijloacelor de socializare pot genera probleme juridice.

X. Lucrări de referință

Ghidul a fost realizat cu sprijinul "The Research Foundation of State University of New York" și suportul financiar din partea Ambasadei SUA în Republica Moldova. Documentul a fost consultat cu reprezentanții societății civile și comunicatorii Guvernului și este recomandat APC-urilor.

Documente consultate:

- *Social Media Standard* from the Office of the State Chief Information Officer from the State of California
- *Social Media Handbook* from the US General Services Administration
- *Social Media Policy* from the US General Services Administration
- *Social Media in Government: Hands-on Toolbox* from New Zealand Department of Internal Affairs
- *Social Media in Government: High-level Guidance* from New Zealand Department of Internal Affairs
- *Best Practices for Social Media Usage in North Carolina* from North Carolina Office of the Governor, Office of Information Technology Services and Department of Cultural Resources
- *Social Networking and Social Media Policy and Standards* from the State of Oklahoma
- *Guidelines for Social Media Usage in United Arab Emirates Government Entities*
- *Designing Social Media Policy for Government: Eight Essential Elements* by the Center for Technology in Government, University at Albany, SUNY