Ghidul de utilizare a rețelelor sociale în sectorul public

Cuprins

I. Cadru general

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

Ghidul de utilizare a rețelelor sociale în sectorul public este **un material de suport** pentru ministere şi departamente, realizat în scopul creării unor proceduri interne de gestionare a utilizării mijloacelor de socializare. Acesta cuprinde următoarele elemente: introducerea, gestionarea contului, crearea conţinutului, implicarea cetăţenilor, 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 şi departamente. De asemenea, acesta se răsfrânge asupra părţilor contractate, antrenate în utilizarea mijloacelor de socializare în numele Guvernului Republicii Moldova, constituind o parte a responsabilităţilor contractuale. Principiile de direcţionare vor fi neutre în raport cu instrumentele utilizate şi vor avea un caracter general aplicabil tuturor mijloacelor de socializare. Ţinând cont de natura dinamică a mijloacelor de socializare, ghidul va fi revizuit şi 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 oportunităţi de transformare a instituţiilor de stat și noi forme de comunicare cu publicul. Instrumentele de comunicare oferite de mijloacele de socializare fac parte din şirul de tehnologii moderne care înlesnesc schimbul interactiv de informaţii, interoperabilitatea, precum şi colaborarea în rândul angajaţilor instituţiilor de stat şi între aceştia şi publicul larg.

Peste 250 de mii de cetățeni moldoveni sunt momentan pe

"Mijloacele de socializare" şi "Web 2.0" sunt termeni generici şi cuprind diverse activităţi, ce integrează tehnologii, interacţiune socială şi crearea conţinutului. Mijloacele de socializare preiau diverse forme, cum ar fi blogurile, wikis (pagini de grup redactate de utilizatori), schimb de fişiere foto şi video, podcasts (distribuire de fişiere multimedia), socializare pe net, aplicaţii tip mash-up şi spaţii virtuale. Mijloacele de socializare reprezintă un set de tehnologii online, pagini, şi practici folosite pentru a face schimb de opinii și experienţă prin antrenarea utilizatorilor.

Facebook. Numărul 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.

Prezenţa pe mijloacele de socializare a unei instituţii de stat a devenit o reflecţie a unui proces de comunicare activ şi transparent. Activităţile de socializare contribuie la îmbunătăţirea interactivităţii dintre o unitate guvernamentală şi publicul pe care aceasta o deserveşte, oferind noi oportunităţi de a accesa segmente de populaţie care nu utilizează mijloace media tradiţionale. Beneficiul de pe urma utilizării mijloacelor de socializare de către instituţiile de stat poate fi unul major, în cazul în care există o strategie de socializare bine gândită. Instituţia guvernamentală va realiza o mai buna transparenţă a activităţilor, o relaţie interactivă cu cetăţenii, o mai mare asumare a responsabilităţilor pentru politicile şi serviciile guvernamentale, astfel căpătând mai multă încredere în rândul populaţiei. Instituțiile publice sunt încurajate să utilizeze tehnologiile de socializare pentru a-şi îmbunătăţi comunicarea, colaborarea şi schimbul de informaţii cu publicul larg, cu alte structuri de stat, cu sectorul privat, cu reprezentanții comunității internaţionale, precum şi cu cetăţenii aflaţi peste hotare.

Instrumentele de comunicare utilizate de instituţiile publice, inclusiv mijloacele de socializare, trebuie să ţină cont de obiectivele de comunicare, colaborare şi schimbul de informaţii. Totuşi, utilizarea mijloacelor de socializare va ţine cont şi de aspectele de securitate, confidențialitate şi profesionalism.

Prezentul document este elaborat pentru a informa angajaţii şi pentru a asigura consecvenţa utilizării mijloacelor de socializare în cadrul tuturor instituțiilor publice. Fiecare structură guvernamentală va perfecta modificările necesare la acest document în funcţie de contextul de serviciu, concomitent oferindu-le angajaţilor sprijin şi 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 şi 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 dificultăţi de ordin tehnic în procesul de creare a unui cont, ulterior pot apărea probleme legate de menţinerea integrităţii conţinuturilor. Astfel, fiecare unitate va avea în vedere proceduri de securitate la crearea contului, identificarea contului şi menţinerea informaţiilor de pe acesta.

Crearea contului

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

Identificarea contului

Orice cont de socializare al unei unităţi guvernamentale va indica clar că acesta este gestionat de unitatea respectivă. Orice cont de socializare gestionat de o unitate de stat va afişa la un loc vizibil informaţiile de contact care să cuprindă cel puţin:

- 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 aceleiaşi parole pentru accesarea mai multor conturi creşte vulnerabilitatea acestor conturi. În cazul în care un administrator de cont pe rețelele sociale va fi înlăturat de la administrarea contului sau destituit din funcţie, partea responsabilă de gestionarea conturilor va modifica imediat parola şi informaţiile de pe cont în scopul menţinerii controlului asupra contului deschis în cadrul instituţiei. Informaţiile noi şi modificările efectuate la cont vor fi puse la dispoziţia părţii 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 conţinutului

Conţinutul de pe conturile de socializare plasat în numele instituţiei de stat şi distribuit prin canalele oficiale de socializare va fi considerat drept informaţie cu caracter oficial. Ţinând cont de aceasta, se impune asigurarea corectitudinii conţinutului pentru a păstra integritatea datelor. Mai mult, limbajul utilizat pe cont va corespunde întocmai limbajului comunicărilor oficiale. Prin urmare, unităţile din cadrul instituţiilor de stat vor desemna părţi responsabile de crearea şi aprobarea informaţiilor plasate pe conturile de socializare bazându-se pe setul minim de cerinţe enumerate mai jos.

Roluri şi responsabilităţi

Fiecare instituției publică trebuie să elaboreze o procedură de autorizare a angajaților cu drept de contribuţie la conţinut. Persoanele cărora li s-au desemnat aceste roluri vor fi responsabile de actualizarea la timp a conţinutului plasat pe contul oficial. Fiecare unitate guvernamentală îşi va elabora o procedură adecvată contextului de serviciu şi va respecta cel puţin următoarele principii:

- Doar funcţionarii autorizaţi vor avea dreptul să plaseze informaţii pe paginile oficiale de socializare, Web 2.0 şi alte reţele de socializare din numele instituţiei de stat. Acest principiu se va aplica în toate cazurile, fie că pagina este gestionată din interiorul instituţiei fie din exterior.
- Angajaţii instituţiilor de stat nu-şi vor exprima opiniile din numele instituţiei pe care o reprezintă pe forumurile neguvernamentale; excepţie vor fi cazurile când plasarea acestor opinii este autorizată de persoana responsabilă de comunicarea pe reţelele de socializare oficiale, de obicei şeful departamentului comunicare.
- Atunci când postează sau fac schimb de informaţii pe forumurile externe de socializare, angajaţii instituţiilor de stat autorizaţi să comunice din numele instituţiei se vor legitima indicând: 1) numele deplin; 2) funcţia; 3) direcţia în care activează şi 4) datele de contact. Postările se vor limita doar la scopul prevăzut de autorizare pentru fiecare caz specific.

Conţinutul

Angajaţii instituţiilor guvernamentale care folosesc mijloacele de socializare pentru a se exprima din numele instituţiei de stat trebuie să ţină cont că afirmaţiile sunt făcute din numele instituţiei. De aceea, aceștia vor face postări sau comentarii echilibrate.

Informaţiile de pe paginile guvernamentale care vor conţine oricare dintre însușirile enumerate mai jos nu vor fi postate:

- Limbaj sau conţinut vulgar;
- Limbaj sau tonalitate ofensive;
- Conţinut care promovează, încurajează sau perpetuează discriminarea pe criterii de rasă, convingeri, culoare, vârstă, religie, statut matrimonial, naţionalitate, dezabilitate fizică sau mintală sau orientare sexuală;
- Conţinut obscen sau link-uri la conţinut obscen;
- Solicitări de afaceri;
- Desfăşurarea sau încurajarea activităţilor ilegale;
- Informaţii care ar putea pune în pericol siguranţa sau securitatea publică sau securitatea sistemelor publice;
- Conţinut care încalcă interesele de proprietate juridică a oricărei alte părţi;
- Promovarea sau opunerea faţă de vreun candidat la funcţie politică sau promovarea sau opunerea faţă de orice plebiscit;
- Utilizatorii nu vor posta sau dezvălui informaţii ce ţin de drepturile de proprietate, date cu caracter confidenţial, informaţii secrete, date personale sau date ce ţin de proprietatea intelectuală a Guvernului.

VI. Implicarea cetăţenilor

Informaţiile care se conţin pe conturile de socializare ale instituţiilor de stat pot veni şi de la publicul larg. Dat fiind caracterul public al reţelelor de socializare şi speranţa la o participare activă din partea cetățenilor, va fi necesar ca instituţiile de stat să-şi elaboreze procedee eficiente pentru gestionarea implicării cetăţenilor, inclusiv desemnarea clară de roluri şi responsabilităţi, norme cu privire la informaţiile postate de cetăţeni şi proceduri de încorporare a feedback-ului din partea acestora.

Roluri şi responsabilităţi

Toate informaţiile din partea publicului vor fi arbitrate de angajaţi autorizaţi ai instituţiei guvernamentale, aceştia fiind instruiţi să monitorizeze şi să răspundă la comentariile şi conținutul plasate de cetăţeni pe reţelele de socializare. Fiecare unitate guvernamentală va desemna o asemenea persoană (sau mai multe) în funcție de contextul de serviciu. Rolurile şi responsabilităţile acestor angajați vor stipula şi intervalul de timp acceptabil pentru a primi postări şi pentru a răspunde la comentarii și solicitări.

Norme privind conţinutul din partea cetăţenilor

Unul dintre cele mai importante obiective pe care instituţiile de stat doresc să-l realizeze prin intermediul reţelelor de socializare este interacţiunea efectivă cu cetăţenii în condiţii

de risc minim. Pentru aceasta, instituțiile de stat sunt încurajate să-şi elaboreze un cod public de conduită pentru utilizatorii publici, cu descrierea comportamentului adecvat din partea cetăţenilor utilizatorilor. Codul trebuie sa fie comunicat explicit pe fiecare reţea de socializare. De asemenea, codul public de conduită va indica clar tipurile de conţinut interzis şi modul în care va fi tratat asemenea conţinut. Codul va aborda cel puţin următoarele aspecte:

- Comentariile irelevante sau ieşite din context.
- Limbajul vulgar.
- Comentariile care promovează discriminarea.
- Comentariile care promovează activităţile ilegale.
- Comentariile care încalcă orice drepturi legale sau drepturi asupra proprietăţii intelectuale.

Normele ce ţin de conţinut vor include şi perioadele de timp alocate pentru a revizui comentariile, postările şi răspunsul instituţiei, pentru a corespunde aşteptărilor publicului.

Angajaţii responsabili de monitorizarea și plasarea răspunsurilor vor fi instruiți corespunzător cu privire la metodele de aplicare a normelor de reglementare a conţinutului. Cenzurarea neadecvată a postărilor va restrânge colaborarea şi participarea publicului. Angajaţii 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 cetăţenilor

Acţiunile de socializare create cu scopul de a antrena publicul în deciziile luate de instituţiile de stat în materie de ghid, ordonanţe şi servicii sau orice alte acţiuni ale Guvernului vor fi bazate pe un şir de procedee, care vor articula modul de încorporare a feedback-ului. Partea responsabilă de monitorizare şi răspuns la feedback-ul publicului va stabili o procedură clară de comunicare cu alte direcţii din cadrul instituţiei de stat, astfel asigurând utilizarea adecvată a feedback-ului solicitat prin reţelele de socializare. Procedura selectată va fi explicată clar şi afişată pe canalul de socializare utilizat de instituţie.

VII. Utilizarea contului de către angajaţi

Utilizarea rețelelor de socializare în cadrul unei instituţii guvernamentale poate fi grupată în 3 categorii: utilizarea de către întreaga instituţie – în acest caz angajaţii folosesc canalul de socializare din numele instituţiei; utilizarea profesională – angajaţii

instituţiei folosesc mijloacele de socializare în scopul dezvoltării profesionale şi utilizarea personală – angajaţii 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 angajaţi şi va stabili limitele adecvate de utilizare. Managerii din cadrul instituţiei vor fi responsabili să comunice regulile de utilizare şi să asigure respectarea acestora de către angajaţi. Fiecare instituţie de stat va aborda cel puţin trei aspecte legate de utilizarea de către angajaţi: accesul angajaţilor, utilizarea admisibilă şi comportamentul angajaţilor.

Accesul angajaţilor

- Fiecare instituţie de stat va stabili în ce măsură va permite angajaţilor accesul la instrumentele de socializare. Accesul poate fi îngăduit tuturor angajaţilor, poate fi limitat în dependenţă de funcţia deţinută sau poate fi permis doar accesul la un număr prestabilit de reţele. 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 reţelele de socializare, instituţia de stat va elabora şi afişa următoarele proceduri:

- Va fi stabilită o procedură prin care angajaţii vor solicita accesul la instrumentele de socializare. Această procedură va detaila următoarele:
  - a) paşii 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 şi în cât timp va fi comunicată decizia solicitantului.

- Va fi stabilită o procedură prin care angajaţii solicită utilizarea unor reţele de socializare specifice. Această procedură va detaila următoarele:
  - a) materialele care trebuie prezentate pentru a sprijini solicitarea de acces a reţelei;
  - b) persoana autorizată să decidă asupra solicitării;
  - c) temeiurile pe care se va baza decizia;
  - d) în ce mod şi în cât timp va fi comunicată decizia solicitantului.

În general, principalul criteriu de aprobare a accesului angajaţilor trebuie sa fie îmbunătăţirea performanţei lor profesionale care să ducă la sporirea randamentului şi rezultatelor produse.

Utilizarea admisibilă

Regulile de utilizare a rețelelor de socializare de către angajaţi sunt similare cu acelea care reglementează accesul la internet, email şi alte TI. Unităţile guvernamentale sunt încurajate să verifice mai întâi dacă pot aplica ghidurile existente şi, 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 instituţiei de stat, angajaţii nu vor avea dreptul să utilizeze reţelele de socializare în scopuri politice, pentru a realiza tranzacţii comerciale sau afaceri personale. Angajaţii trebuie să ţină cont că utilizarea necorespunzătoare a mijloacelor de socializare poate servi drept temei pentru acţiuni disciplinare. Normele de utilizare admisibilă trebuie să cuprindă următoarele arii:

- **Utilizarea din numele instituţiei.**
  Angajaţii responsabili de menţinerea prezenţei instituţiei pe reţelele de socializare au dreptul să le utilizeze în beneficiul instituţiei. Acest lucru presupune monitorizarea forumurilor sociale relevante, menţinerea prezenţei instituţiei pe reţelele de socializare şi monitorizarea tendinţelor şi a practicilor optime de utilizare a reţelelor de socializare în instituţiile 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 reţelele de socializare în vederea îmbunătăţirii performanţei profesionale va automonitoriza utilizarea pentru a se asigura că activităţile de pe canalele de socializare contribuie la creşterea profesională şi nu o împiedică. Abilităţile căpătate de un angajat în urma utilizării reţelelor de socializare în timpul orelor de lucru trebuie sa fie direct legate de sarcinile şi atribuţii prevăzute de fișa de post.
- **Utilizarea contului în scopuri personale.** Angajaţii 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. Angajaţii 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 angajaţilor

Comportamentul angajaţilor pe reţelele de socializare în timpul orelor de lucru va fi reglementat de normele existente privind conduita la locul de muncă. Angajaţii vor manifesta precauţie cu privire la informaţiile lor personale sau profesionale afişate pe reţelele de socializare. Toţi angajaţii, indiferent de gradul de acces la mijloacele de socializare, vor respecta următoarele reguli generale:

- Angajaţii care accesează reţele de socializare prin intermediul conturilor deschise de instituţia de stat şi care se exprimă din numele instituţiei, vor respecta toate normele ce ţin de comportamentul inadmisibil la locul de muncă, inclusiv ghidurile privind comportamentul admisibil, acordurile de utilizare, prevederile referitoare la hărţuirea sexuală, etc. Toate informaţiile comunicate prin reţelele guvernamentale vor avea caracter profesional şi vor respecta ghidurile, normele şi aşteptările instituţiei cu privire la comunicare.
- Angajaţii instituţiei de stat vor putea să-şi includă funcţia oficială pe conturile personale de pe reţelele de socializare. În acelaşi timp, funcţionarii care nu sunt autorizaţi să se exprime din numele instituţiei vor menţiona clar că toate activităţile şi comentariile de pe reţelele de socializare nu reprezintă în niciun fel poziţia oficială a instituţiei. Termenii de utilizare vor fi clar afişaţi pe fiecare pagină de socializare.
- Angajatul instituţiei de stat va răspunde de acţiunile sale pe reţelele de socializare asigurând că acestea nu cauzează niciun prejudiciu imaginii instituţiei.

VIII. Aspecte privind securitatea

Reţelele de socializare prezintă riscuri de securitate. De aceea, unităţile guvernamentale vor întreprinde toate măsurile posibile pentru a-şi proteja canalele de comunicare, infrastructura şi informaţiile private şi confidenţiale despre angajaţi și public. Cele mai frecvente modalităţi de a ataca securitatea reţelelor sociale includ phishing-ul datelor de autentificare, tehnici de manipulare – social engineering, falsificarea identităţii – spoofing şi atacarea aplicaţiei web. În acelaşi timp, paşii accelerați cu care se dezvoltă tehnologiile informaţionale impun necesitatea actualizării continue a protocoalelor de securitate pentru a face faţă noilor ameninţări de securitate. Prin urmare, fiecare unitate guvernamentala îşi va educa angajaţii privind riscurile asociate utilizării reţelelor sociale şi modalităţilor de atenuare a acestora. În general, utilizarea paginilor de socializare va fi reglementată de normele de securitate curente, aplicate la întregul sistem de tehnologii

informaţionale. Pe lângă ghidul privind securitatea informaţională, instituţia va mai întreprinde următorii paşi:

- Angajaţilor nu li se va fi permite să utilizeze adresa de email sau parola de la locul de muncă pentru a-şi accesa conturile în reţele de socializare.
- Angajaţii nu vor avea "privilegii de administrator" pe calculatoarele de serviciu cu acces la internet.
- Direcţia tehnologii informaţionale din fiecare unitate de stat va revizui tehnologiile selectate, clienţii și plugins-urile cu scopul de a preveni vulnerabilitatea sistemelor informatice înainte de utilizarea acestora.
- Pentru a menţine securitatea utilizatorilor şi a parolelor în reţeaua instituţiei, persoanele autorizate cu acces la reţele de socializare vor folosi nume de utilizatori şi parole diferite de cele aplicate în reţeaua 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 autorizaţi îşi vor configura mijloacele de socializare, Web 2.0 sau clienţii din reţelele sociale, blocând mesajele de la surse neautorizate.
- Angajaţii trebuie să ştie ce date pot sau nu pot fi diseminate.
- Utilizatorii din cadrul unităţii guvernamentale vor fi instruiţi în materie de securitate informatică şi anume în sfera riscurilor generate de divulgarea datelor pe reţelele de socializare şi mecanismelor de atacare a securităţii.
- Utilizatorii din cadrul instituţiilor guvernamentale vor fi instruiţi cu privire la ghidurile de utilizare şi securizare a mijloacelor de socializare, fapt care îi va ajuta să-şi controleze mai bine propria securitate şi să se protejeze mai eficient contra dezvăluirilor neatente de informaţii de serviciu sensibile.
- Înainte de a autoriza accesul pe paginile de socializare, utilizatorii din cadrul instituţiilor guvernamentale vor fi instruiţi cu privire la ameninţările specifice asociate reţelelor sociale.

IX. Aspecte de ordin legal

Accesul la paginile de socializare şi utilizarea lor în cadrul unităţilor de stat vor fi reglementate prin legi, ghiduri şi proceduri existente şi aplicabile, inclusiv **acelea** privind securitatea informaţională. Toate tipurile de utilizare vor respecta aceste reguli precum şi normele prevăzute de acest document. Utilizarea mijloacelor de socializare în cadrul unei instituţii guvernamentale poate duce la apariţia unui şir de probleme de ordin legal. Majoritatea acestora sunt evitate prin exercitarea de bun simţ și respectarea normelor existente de conduită. În acelaşi timp, este important să se clarifice parametrii juridico-

legali în care operează instituţia, mai ales ţinând 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 şi 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