United Arab Emirates

حكومة الإمارات الإلكترونية
Emirates eGovernment

Guidelines for Social Media Usage

in

United Arab Emirates Government Entities

Version 1.0

January, 2011

This document was developed as part of the Web Technical Guidelines Document for UAE Government Entities

This document was developed in partnership between:

حكومة الإمارات الإلكترونية
Emirates eGovernment

&

كلية دبي للإدارة الحكومية
DUBAI SCHOOL OF GOVERNMENT

For any inquiries please contact:

Mr. Ibrahim Elbadawi

Strategic Planning Specialist

Ibrahim.elbadawi@gia.gov.ae

Acknowledgement

A special acknowledgment to:

- UAE Government Entities for their participation in the development of the first draft of this document through the policy forum and roundtable sessions and for their continuous feedback.
- Mr. Andria Di Maio, *VP Distinguished Analyst – Gartner Inc.* for his valuable contribution in formulating the guidelines throughout the multiple stages of the process.
- Mr. Richard Kerby, *Senior Inter-Regional Adviser (DPADM/UNDESA) – United Nations* for his input in aligning the guidelines with the expectations of United Nations eGovernment Development Model.
- Center for Technology in Government, University at Albany - Albany, New York. Its 'Designing social media policy for government: Eight essential elements' report was a very valuable tool for developing this document.
- And for citizens and residents of United Arab Emirates who participated in the policy forum dedicated to develop the first draft of this document.

TABLE OF CONTENTS

1. PURPOSE OF THE DOCUMENT

This document provides the government entities in the United Arab Emirates (UAE) with policy guidelines on how to use Social Media (SM) tools in responsible, safe and effective manners to communicate with their clients and public and engage them in designing/delivering government programs and services.

According to a national survey, strong realization of the usefulness of social media already exists among employees of the federal and local UAE government sectors.[1] Many federal and local government entities across UAE have already started using social media tools as a mean of communication with the public, however, most if not all of these entities lack guidelines or policy instructions that could help them leverage the benefits of social media and avoid their potential risks and threats.

2. SCOPE OF THE DOCUMENT

The scope of this guidelines document is defined as follows:

- It's applicable to all UAE federal government entities (ministries, authorities and programs) and local government entities.
- The document covers social media tools defined in the Glossary section which cover for example social networking sites (e.g. Facebook), Wiki tools and blogs. Some of these tools could be government-owned (e.g. government blog) while some of them might be commercial sites (e.g. Facebook).
- The guidelines presented in this document are tool-neutral, guidelines on how to use specific social media tools and sites (e.g. Facebook) will be provided online[2].
- In keeping with the dynamic nature of social media, this guidelines document will evolve and change as needed.

3. INTRODUCTION

Social media tools with their collaboration and participation capabilities have eclipsed the static, publish-and-browse Internet and become a new force that could shape the future of governments through reinventing their structures and public services.[3]

More specifically, social media "can help policy makers set priorities, encourage more citizens to 'buy in' to programs, increase satisfaction levels and thus augment the chances of successful policy outcomes. For example, social networking sites such as Facebook, YouTube and Twitter, as well as blogging software and mobile technology, allow governments to tap into the collective knowledge of society quickly and directly. In this way, citizens move from being passive consumers of government services to advisers and innovators contributing ideas that are in better accord with their individual and group needs"[4].

The popularity of social media sites has been increasing remarkably, the number of subscribers at Facebook alone has exceeded 500 users.[5] Locally, the UAE is ranked first among Arab countries with 45% of its population owning Facebook accounts, in addition to being among the top 10 countries in the world in terms of Facebook penetration.[6]

Along with these clear benefits, the fundamental changes in government and their relationship with the public sparked by social media tools could pose several challenges and threats that need to be carefully considered and tackled.

There are several methods of utilizing social media tools within government. One such classification[7] is:

- **Inward Sharing** – of internal organizational documents within and between government entities.
- **Outward Sharing** – of information and documents with other government entities, organizations and individuals through government websites.
- **Inbound Sharing** – which is similar to 'crowdsourcing' or conducting a large online poll on a government website.
- **Outbound Sharing** – which consists of engaging with the public through existing commercial websites, and which will be the main focus of this document.

3.1. Risks

While using social media tools has its benefits, one must assess the related risks as well. These include:

- Negatively affecting employee productivity;
- Tying up network bandwidth;
- Creating reputational damage to individuals or government entities;
- Potentially leaking private or sensitive government or personal information
- Security risks such as spear phishing, social engineering and possibly introducing malware, viruses, etc…and other security breaches.

3.2. Risk Mitigation:

These risks can be mitigated by applying the proper controls, some of these controls include:[8]

Policy controls: These outline appropriate behavior and content guidelines when using social media tools such as the ones outlined throughout the different sections of this document.

- Acquisition controls: Examples of these can be found in the 'Access to Social Media Websites' section. They allow for greater security and privacy settings and greater control of information (such as setting strict authentication measures or managing cookies) when subscribing to commercial social media sites.
- Training controls: These provide awareness and courses for employees on policy, conduct and best practices when it comes to using social media tools.

4. GUIDELINES IMPLEMENTATION REQUIREMENTS

While most of the government entities in UAE are used to the implementation of some organizational policies such as IT related policies, social media related policies and guidelines represent unchartered territory for them. The successful implementation of this social media guidelines document requires the government entities to handle the following arrangements:

- Assigning the responsibility of promoting this document, monitoring the compliance with its contents, and dealing with all aspects related to social media to a specific organizational unit within the entity. It's up to each entity to pick the most appropriate unit for its needs. The list of such units includes but is not limited to: the Media or Public Relations unit, the Human Resources department, the Information Technology (IT) department, the Knowledge Management department or a joint committee between these departments.

- In all cases, government entities should not permanently outsource this responsibility to outside vendors or third parties.
- As most of the activities on social media websites involve engaging the public in taking decisions on some of the government policies or services, the selected unit needs to establish a clear communication process with other units inside the government entity that is responsible for designing or delivering these policies/services. In addition, this unit should develop the indicators to measure government employees' performance and the impact of engaging with the public through social media tools. .
- In parallel to the implementation of this policy, government entities must have continuous educational and awareness raising programs to boost the employees' understanding of social media benefits and threats and their ability to properly comply with the guidelines detailed in this document.

In addition, government entities are urged to review and update their strategies, decision making mechanisms and service design and delivery processes to ensure leveraging the public participation offered through social media and measuring the impact of adopting these social media tools.

5. GUIDELINES FOR SOCIAL MEDIA USAGE

Following are the detailed guidelines for usage of social media tools by government entities. These guidelines cover eight areas: Access to Social Media Websites, Account Management, Employee Conduct, Content Management, Privacy, Security, Other Legal Issues and Public Code of Conduct.

5.1. Access to Social Media Websites:

This article tackles the issue of accessing social media websites during working hours or using the government's resources (e.g. computers). Some government entities tend to grant access to social media sites to only some of its employees in addition to developing a list of the accessible websites.

Although government entities may vary depending on the nature of their services and the nature of their relationships with the public, the following requirements should be maintained in all cases:

- The main driver behind granting access to employees is to ultimately enhance their work performance and contribute to improving their outputs and deliverables.
- In general, employees access social media websites during working hours for the following three reasons:
    - To manage the entity's official account on social media websites.
    - To fulfill work-related interests through their personal accounts on social media sites.

   - To use these websites for personal or non work-related interests.

- It should be noted that the lines between personal and professional usages of social media sites are blurry, making the issue of granting access to one rather than the other difficult.
- In principle, access to social media sites shouldn't be banned and they should be used in compliance with this guidelines document and with the existing code of conduct. As such, employees should be held accountable for any improper use of any social media site.
- Banning employees from accessing social media sites might not be effective as they can access it through other channels including their mobile phones.
- Because of the dynamic nature of social media, a list of recommended websites should be developed and updated by the Social Media Unit periodically in a collaborative, rather than top-down manner, with the employees themselves, and with input from all related organizational units including but not limited to the IT unit. This list should consider the benefits and risks of social media websites as identified in the introduction part of this policy, with good practices for usage disseminated.

5.2. Account Management

The process of managing an account on social media websites covers several aspects, often referred to as 'life cycle management', including:

- Creating;
- Maintaining; and

- Deactivating or deleting accounts as appropriate, depending on the type of account and its function, outlined below.

Depending on the social media website, the creation of an account gives the creator access to a variety of communication and collaboration tools such as: posting comments and multimedia content, chatting, blogging, connecting with other users etc… As mentioned in the previous section, there are two types of accounts that employees may have on social media websites; outlined below are the details on managing these accounts:

Managing the Entity's Official Accounts on Social Media Websites:

In this case, a government employee is authorized to officially communicate with the public over social media websites on behalf of the entity. All the comments and views posted by this employee represent the official point of view of that entity. The following guidelines should be fulfilled:

- The decision of creating an account on a social media website as the entity's official account should be approved by the social media Unit. However, before taking such decision, the Social Media Unit must consult the IT unit to cover any technology-related risks or and refer to them on issues such as monitoring privacy settings; other relevant units should be consulted as well. This approval should take in consideration factors like the suitability of the site to the government entity needs and target audience in addition to any technology-related factors.
- This decision must be written and must identify in addition to the specific social media website, the name and position of the employee(s) who will be responsible for managing

this account. Also, the decision should specify the exact policies or services that the employee can interact with the public on via that account.

- When selecting the employee to manage the account, several requirements should be taken into consideration including:
  - His/her level of qualification and understanding of the issues to be communicated and discussed with the clients and public on social media sites.
  - His/her language and communication skills.
  - His/her level of awareness with social media sites and familiarity with methods of communication on them.
  - His/her readiness to stay online on the social media sites beyond the government working hours and his ability to act in the situation that needs immediately respond in such times.
- When given the authority to use their names to represent the entity on social media sites and communicate on its behalf, employees should identify themselves by: Full Name, Title, Entity, and Contact Information.

Managing the Employees’ Personal Accounts for Work-Related Interests:

Employees might access social media websites to search for information or news that is necessary to fulfill their job responsibilities (or for personal interests, as explained in Section 5.1). In this case, they can leverage the resources and information provided on social media sites to deliver their daily tasks and duties. As employees are responsible for managing their personal accounts, they are expected to conduct themselves as per section 5.3 (Employee Conduct).

5.3. Employee Conduct:

In essence, the conduct and behavior of the government employees on social media websites shouldn't differ from their behavior in general or any other communication/media tool which is mainly governed by the document of Professional Behavior Principles and Ethics in the Public Office of Federal Authorities[9] issued in July 2010, and the UAE Human Resources law (Federal Law Decree #11 for the Year 2008)[10]. This doesn't only cover the employee behavior on social media websites but also the "acceptable use" of government resources and information, this includes for example:

- To behave in a way which preserves the reputation of the government in general and the entity in which he works, in particular.
- To observe the finest moral principles in the behavior and conduct of the employees.
- To use public funds in an honest and transparent manner and avoid wastage.
- Not to use the information obtained during performance of his job duties for other non-work related purposes.

In addition to these requirements and to assure distinction between their professional positions and their personal activities and views, government employees must comply with the following policy guidelines when using social media websites on their personal capacity whether to fulfill work-related or personal needs:

- On their personal profiles (if any) on social media sites, government employees shouldn't post their official contact details for correspondence. This includes: email, phone number, post office number etc…

- Government employees can mention their official title in their personal profiles, in this case they must put a clear disclaimer, developed by the official legal department and made available to employees, clarifying that their activities and comments on the social media website represent their personal views only and not related to their government.
- In all cases, it is the government employee's responsibility to ensure that his/her personal behavior on social media websites does not harm the reputation of the government entity or any other entities in any way.

5.4. Content Management:

A government entity is responsible for continuously publishing and managing the contents of their pages on both government-owned and commercial social media websites. This responsibility should be assigned to the organizational unit that is responsible for publishing and managing the entity's content on "traditional media" unit but the following characteristics of social media must be taken in consideration:

- Communication with the public on social media websites tends to be interactive rather than authoritative and tends to be narrowcast as compared to the broadcast traditional media which means that the right message from government organization can be sent quickly and directly to the right audience[11].
- Promoting a collaborative environment is key to creating successful online communities that will participate in a meaningful dialogue and contribute to a productive public engagement.

- The great portion of content posted on social media websites is User Generated Content (UGC) which raises a valid concern about the reliability of this content and the challenge of moderating this UGC or governing the participants' behavior.
- The pattern of discussions on social media websites is spontaneous, informal and unpredictable .
- Unlike the government working hours, participants on the entity's page on a social media websites can keep updating it around the clock.

In light of these characteristics, government entities need to take decision on the following issues:

- The selection of the employees who will manage the content of on the entity's account and interact with the public. The above characteristics of social media along with the advises provided on section 5.2 (Account Management) can help in making this decision.
- The 'Life Cycle Management' of the content posted on social media websites, managing the deletion/removal of any information that might become irrelevant for any reason such as the leave or resign of contact employee at the entity.
- The moderation strategy (if any) to be adopted by the entity to manage the UGC. Moderating the UGC is important to ensure proper conduct. It should be done carefully so as not to restrict said collaboration and participation, and should be clearly communicated to users to set their expectations and guide their contributions. Mainly, if the user's contribution is within the context of the topic of discussion, regardless of

whether it is positive of negative, it should be allowed to remain. However, if the content is offensive, derogatory, or completely out of context then it may be removed.

There are several types of moderation to choose from:

- **User-moderation:** Where it is left up to the user to self-censor according to a code of conduct that should be explicitly posted on the website. This is the least restrictive form of moderation and requires the minimal resources, but would constitute the largest amount of risk for posting inappropriate content.
- **Community-moderation:** An example of this is 'Report Abuse' functionality, which will allow the administrator to assess reports from users on inappropriate content and take suitable action.
- **Administrator – moderation:** the administrator monitors all content as it is posted and has the right to remove content if it violates certain criteria (see Section 5.7 – Public Code of Conduct).
- **Content pre-moderation:** (i.e. screening every posting before allowing it to go live), which would allow for greater control but would also slow down the exchange/discourse between people and may lead them to leave the site. It would also require considerable resources.
- **Content post-moderation:** in which the government entity allows users to post comments on a their SM page and be immediately displayed, only intervening afterwards if any abuse is reported.

- **Automated Moderation:** in which a filter is set up to automatically flag combinations of keywords that have been classified as spam by the moderators, after the which the content is then manually reviewed to assess its appropriateness.

5.5. Security:

As highlighted in the introduction part, security is one of the major concerns related to social media websites. These sites such as blogs, social networks and Wikis are exposed to three different types of security threats: Spear phishing, Social Engineering, and Web Application Attacks (see Appendix A - Glossary for Definitions).

In general and where appropriate, current IT security policies shall apply to social media websites as well but in addition to this, the following actions must be taken by the entity:

- Ensuring employees do not use their government official email address or password to sign in to their accounts in social media websites.
- Preventing access to unnecessary functionalities and applications within some of the social media websites , because of security risks such as spam, phishing and security attacks.
- Educating employees about these security threats especially the social engineering related threats and the risk mitigation techniques.

5.6. Privacy

Similar to the security threats, engaging on social media websites increases the chances of privacy breaches – that is the inappropriate use of government information by those who are not allowed to have access to this information. While UAE has not yet approved an online privacy law, government entities should take all the necessary actions to ensure protecting the privacy of government data and information against possible privacy threats created by social media websites. At the minimum level, the following policy requirements should be implemented:

- Government entities should clearly specify the type of information that can be disclosed by its employees on social media websites.
- Employees shouldn’t assume privacy on social media websites. Comments posted on these sites will stay there for long time and are accessible by the visitors of these sites and sharable on other sites even without necessarily asking for the author’s permission. Consequently, employees should be vigilant when posting or providing information on social media websites in order to protect both:
    - Their own personal information; and
    - Sensitive government information such as confidential data or private information about its clients.

5.7. Public Code of Conduct:

One of the main objectives of utilizing social media websites is for governments to engage with clients and the public, and to do this effectively and with minimal risk, a public code of conduct outlining appropriate behavior for users should be developed, and it should be clearly positioned on the site for easy referral.

For example, the public code of conduct can explicitly state that certain forms of content are prohibited and will be removed, including, but not limited to:

- Comments that are out of context or irrelevant.

- Profane language.
- Comments that promote discrimination.
- Comments that promotes illegal activity.
- Comments that violates any legal or intellectual property rights.

5.8. Other Legal Issues:

The use and management of social media websites raise valid concerns about the legal concepts of copyright and intellectual property ownership. The ease of copying and sharing content on social media websites makes it very easy to unintentionally breach copyright laws.

On the government page on social media websites, the government entity must post a clear disclaimer to retain the copyright of government-generated content and must refer to the United Arab Emirates Copyright Law 01/07/2002-1423, No. 7. The disclaimer should also detail the copyrights that non-government contributors to their sites may retain.

After all, government entities must always realize the difficulty of protecting the copyright of the content published on social media websites. Therefore, they should carefully select and review any content to be published on social media websites before publishing it to ensure the protection of government data and information.

Even when copyright is established and protected, another legal issue to take into consideration down the line is the issue of storing and retaining the information on social media websites, and whether or not this information would be considered public record, thereby allowing it to be open and accessible to everyone. Most government information is considered public record, and information posted on government sites or by government employees on social media websites could be classified as the same. Clarifying and defining these distinctions will help to establish how to handle, store and dispose of the information in the long term.

6. GLOSSARY

Social Media: is media for social interaction, using highly accessible and scalable publishing techniques. Social media use web-based technologies to transform and broadcast media monologues into social media dialogues. They support the democratization of knowledge and information and transform people from content consumers to content producers.[12]

Social Media Unit: in this policy document, we use this term to refer to the organizational unit that is responsible for managing the government entity’s presence on social media sites and taking all the social media related decisions. We recommend this unit to be the media or public relationship unit but it’s up to each entity to pick the unit that considered the most appropriate one for its situation.

Government Entity: any government organization in United Arab Emirates including ministries, authorities, departments and programs on both federal and local levels.

Government-owned Social Media: social media tools or sites that are owned by a government entity such as a blog on a government website.

Commercial Social Media: social media sites that are not owned by a government entity, examples of this include social networking sites (e.g. Facebook) or a blogging website (e.g. WordPress).

Spear Phishing: an attack targeting a specific user or group of users, and attempts to deceive the user into performing an action that launches an attack, such as opening a document or clicking a link.[7]

Social Engineering: a security threat which relies on exploiting the human element of trust by collecting some personal information about the target. Such information could be collected from the user account on social media sites. [7]

Web Application Attacks: Web Applications are dynamic web pages that use scripting to provide additional functionality to the user. Social media websites are advanced web applications, as their use requires a high level of interaction and capabilities. This opens up social media websites to a wide range of vulnerabilities exploitable by attackers. [7]

Social Networking Sites: online tools that allow users to (1) create profiles, (2) connect with other users within the boundary of the network, (3) engage in joint discussions and collaborative activities with those connected users and (4) post user-generated content in many formats such as text notes, photos, videos etc…[13]

Blog: a portmanteau of the term "web log" - is a type of website or part of a website. Blogs are usually maintained by an individual with regular entries of commentary, descriptions of events, or other material such as graphics or video. Entries are commonly displayed in reverse-chronological order.[14]

7. REFERENCES

1 Salem, F., Jarrar, Y. (2010). Government 2.0. Technology, trust and collaboration in the UAE public sector. Policy & Internet, 2(1), 4.

[2] Will be available later through EMIRATES EGOVERNMENT website for (Emirates eGovernment.gov.ae). Meanwhile, you can use the available online resources.

[3] World Economic Forum (2009). The Global Agenda 2009. Geneva, Switzerland

4 United Nations. (2010). United Nations e-Government survey 2010, leveraging e-Government at the time of economic and financial crisis. (Tech. Rep. No. ST/ESA/PAD/SER.E/131). New York, United States: United Nations.

[5] Facebook.com, retrieved on January 28, 2011.

[6] Mourtada, R. & Salem, F. (2011). Arab Social Media Report. Dubai School of Government: http://www.arabsocialmediareport.com/

[7] Federal CIO Council (2009). Guidelines for Secure Use of Social Media by Federal Departments and Agencies. United States.

[8] Hrdinová, J., Helbig, N., & Peters, C. S. (2010). Designing social media policy for government: Eight essential elements. Albany: Center for Technology in Government.

[9]http://www.wam.org.ae/servlet/Satellite?c=WamLocEnews&cid=1278055811719&p=1135099400228&pagename=WAM/WamLocEnews/W-T-LEN-FullNews

[10] Can be accessed on: http://www.fahr.gov.ae/assetsmanager/Files/HR_LAW-eng.pdf

11 Hrdinová, J., Helbig, N., & Peters, C. S. (2010). Designing social media policy for government: Eight essential elements. Albany: Center for Technology in Government.

[12] http://en.wikipedia.org/wiki/Social_media

[13] Al Shair, S., Elbadawi, I. (Forthcoming). Social Network Sites and e-Governance: Designing Effective Policies for Government Organizations.

[14] http://en.wikipedia.org/wiki/Blog