Setting up of social media accounts for Ministries and Departments

1. INTRODUCTION

The Republic of Mauritius has, over the years, initiated various computerisation and infrastructure projects to empower civil servants with better tools to serve the nation and to develop ICT awareness. The context has gradually evolved, with ICTs being adopted globally as vital tools to tackle the traditional challenges of human and social development. It is imperative to engage and promote dialogue, using ICT as facilitator, between the different stakeholders.

Social Media offers new opportunities for better communication and knowledge transfer among Government officers, policy makers, service delivery units and the public at large (Government of India, 2012). Thus, the elaboration of a series of recommendations and framework is needed to assist the different Ministries and departments in the setting up of their social media accounts.

2. AVAILABLE PLATFORMS

There are numerous social media platforms that each serve a specific purpose, and address a specific profile of the population. Three main platforms have been identified as being the most accessible, popular and able to serve the public bodies' purposes.

2.1. Facebook

Facebook is a social networking website that has over 900 million subscribers. It has had a huge impact on modern society, including Mauritius, where a very high ratio of young people and adults regularly connect and share content with each other.

2.2. Twitter

Twitter is an online micro-blogging website with 300 million active subscribers. Twitter does not have the same appeal to Mauritians as Facebook; however, tourists and foreign nationals regularly use twitter to stay abreast of general news and updates from their friends and family.

2.3. YouTube

YouTube is an online video sharing website that can be used to broadcast information and updates to the public. Examples would include explanations on government policies, campaigns, and updates on government projects, thus promoting transparency and citizen empowerment.

3. TECHNICAL SECTION

This section describes the technical and other considerations.

3.1. Hardware Requirements

To implement social media presence for the public body, there are no additional hardware requirements, other than the availability of a computer, a modern Internet browser and an Internet connection. The table below gives an indication on the recommended requirements for accessing all of the social media platforms.

Requirements	
Computer	
CPU Speed	2.33GHz or faster x86-compatible processor
Memory	2Gb RAM
Operating System	Windows 7+ / Mac OS X 10.7+ / Ubuntu 10+ / Linux OS 11+ (64-bit)
Browser	
Browser name	Mozilla Firefox/ Safari/ Google Chrome/ Internet Explorer/ Opera
JavaScript enabled	Yes
Adobe Flash Player	Yes
Internet Connection	
Broadband	Yes
Speed	1Mbps

Table 1 Recommended system requirements

During implementation of social media accounts, it is recommended that the computers at the public body are assessed to ensure that they are sufficient for social platform management as well as basic photo and video editing for the purposes of uploading and sharing media content.

3.2. FACEBOOK PAGE

3.2.1. Setting up of Facebook page

A Facebook page is required to disseminate information to the public and to interact with them. Sensitization campaigns can also be posted on the Facebook page and this will help to share important information with the public.

3.2.2. User roles in Facebook management

5 different types of roles for people can be adopted to manage Pages. The table below outlines these roles:

	Admin	Editor	Moderator	Advertiser	Analyst
Manage Page roles and settings	✓				
Edit the Page and add apps	✓	✓			
Create and delete posts as the Page	✓	✓			
Send messages as the Page	✓	✓	✓		
Respond to and delete comments and posts to the Page	✓	✓	✓		
Remove and ban people from the Page	✓	✓	✓		
Create ads	✓	✓	✓	✓	
View insights	✓	✓	✓	✓	✓
See who published as the Page	✓	✓	✓	✓	✓

Table 2 Adapted from Chart Courtesy of Facebook © 2012

It is suggested that the public bodies make use of the above table to assign different roles to users.

3.2.3. Account Management

- All accounts should designate a back-up for if/when the designated individual is sick or on vacation, or if there is an emergency.
- When a designated individual leaves his or her position, the user's access to the account should be terminated immediately. A replacement should be found in

advance of the individual departure. In addition, the password connected with the account should be changed.

Administrative credentials are user accounts that are authorized to perform system and security related functions that ordinary users are not authorized to perform. Example of system and security related functions include creating/updating other user accounts.

Below are some recommendations to effectively secure administrative/privileged credentials.

- Strong Authentication

It is necessary for administrative credentials to adopt stronger passphrase complexity requirements. It is recommended that Administrative accounts use longer passphrase of ten (10) characters or more and contain characters from two of the following three character classes:

  - Alphabetic (e.g., a-z, A-Z)
  - Numeric (i.e. 0-9)
  - Punctuation and other characters (e.g., !@#$%^&*()_+|~-=\`{}[]:";'<>?,./)

- Keep password secret

Password should not be shared your password. Moreover, MYS should consider not giving passwords and administration rights to occasional social media contributors, and temporary workers like interns and passwords be stored in one common, safe location.

- Keep environment updated and protected

  - Always ensure that the software in use is up-to-date. Not only does this include the operating system and web browser, but also third-party plug-ins, such as PDF viewers.
  - Install all the latest patches and hot fixes from the official site and automatically check for newer available versions through the software.
  - Use comprehensive security software to protect against these threats.

- Avoid High Risk Activities
  - Create separate non-administrative accounts to perform activities that do not require administrative privilege, such as reading and editing general

comments.

- Use administrative credentials only to perform application specific functions that require administrative privilege.
- Logout from administrative accounts when not in use.

3.2.4. Content Management

Social media is very time intensive. To ensure both responsiveness and consistent content generation, multiple administrators should monitor the account to ensure regular content posting and audience engagement.

Also, once an account is established, it will not be appropriate to leave the same without any activity as this would reflect poorly on the Ministry.

3.2.5. Moderation of user posts/comments in Facebook

The public body should have moderators who will be reviewing and approving comments from members of the public before it can be published.

Moderation will consist of the following items:

- Moderate posts to the page, comments from fans and the general public
- Block certain words from appearing on the page and turn on the profanity filter
- Respond to comments from the public in a reasonable time
- Ban a person for continuous misbehaviour
- Delete harmful comments
- Confidential information and copyrighted material must not be divulged without proper authorisation
- Establish an escalation mechanism for responding to queries
- Setup alert mechanism for comments

The Facebook page can contain a disclaimer to prevent abusive language or other types of potential misuse from the public.

3.2.6. Legal consideration

- Crediting sources, when reposting or borrowing content from an external source (For example, Image copyright)
- Privacy and disclosure procedures
  Define what is considered confidential and non-sharable
- Employee disclaimers
  Require employees to include a disclaimer when publicly commenting on content related to your business that identifies them as an employee.

3.3. TWITTER ACCOUNT

3.3.1. Setting up of a Twitter handle

A twitter account will be setup for the public body, which will cover important information, updates and links to educational content. As with Facebook, sensitization campaigns can also be posted on the twitter account.

3.3.2. Managing the Twitter account

The management of a Twitter account simpler than that of a Facebook page. Upon creation of an account, the public body will need to provide a bio to let its audience know what is the mission and scope of the organisation's work. The next step is to start providing content, which is the main focus of the Twitter platform.

To allow multiple users to manage and post updates, Twitter has provided a tool called TweetDeck, which allows multiple users to log in and post updates, while reviewing a maximum of information from different sources at the same time.

The Twitter bio can contain a link to a disclaimer to prevent abusive language or other types of potential misuse from the public.

3.4. YOUTUBE CHANNEL

3.4.1. Setting up of a YouTube channel

YouTube channels are excellent ways to provide educational information regarding awareness and readiness in case of disasters. Videos are hosted on YouTube servers, which usually have a high availability and broadband ability as compared to privately owned servers. To create a channel and start uploading videos, the public body needs to create a Google account first.

3.4.2. Managing the YouTube Channel

The setting up of the YouTube channel also includes the option of either creating a standard YouTube channel or setup a Google+ profile and create a linked YouTube channel.

A Google Account is specific to just one person, so it uses one name and identity across all Google services, including on any YouTube channel that is connected.

	Standard YouTube account	**Google+ linked to YouTube channel**

Account ownership	One person owns the YouTube account	Each Google+ profile is owned by one person
Account management	Single account, single channel	Each Google+ profile can manage many channels and each channel can be managed by multiple Google+ accounts

Table 3 YouTube account description

The YouTube page can contain a disclaimer to prevent abusive language or other types of potential misuse from the public.

4. TRAINING

4.1. Technical training

The public body will need to train its staff on how to use the social media platforms; e.g. how to review comments/posts from the public.

At this point, the Central Informatics Bureau can identify the type and nature of technical training sessions.

4.2. Public relations and communications training

Awareness regarding public relations and user engagement will also be required to ensure that the social media platforms remain active and relevant to expectations of the general public.

5. WAY FORWARD FOR SOCIAL MEDIA USAGE

5.1. Social Media Profiles

It is important to identify the proper Public Relations staff to maintain and manage the social media accounts, as they will be the voice and ears of the Ministry/Department vis-à-vis the Mauritian Internet users.

In order to implement and follow-up on social media interactions, the following profiles are suggested:

- **Social Media Manager:** A Social Media Manager is a person in the Ministry/Department well versed in public relations/communication who will be able to redact, approve and edit content such as communiqués, news and updates. The Social Media Manager should also be aware of copyright and confidentiality restrictions, including when sharing of multimedia content such as photos, videos and sound clips. The Social Media Manager should also be aware of language constructs (e.g. use of emojis, hashtags and even memes to convey emphasis on the information being published) and other differences when talking to the public

  It is suggested that a social media manager identified for each Ministry/Department be given the admin/manager roles for Facebook, Twitter and YouTube.

- **Social Media Moderator:** The Social Media moderator is a staff that can assist the social media Manager in his/her duties, including writing draft content. Approval of content for posting can be reserved to Social Media Managers.

  It is suggested that two staff in each Ministry/Department be given the moderator/backup manager roles for Facebook, Twitter and YouTube. The roles are summarized in the following table.

Profile	Role on each Platform		
	Facebook	**Twitter**	**YouTube**
Social Media Manager	Admin	Account owner	Channel manager (via Google+)
Social Media moderator (x2)	Editor	Account owner (shared)	Channel co-manager (via Google+)

Table 4 Role description for each Social Media Platform

5.2. Social Network guidelines

Regarding social media setup, a general set of guidelines has been compiled below, so that they may be considered and adapted in the public bodies' context. These guidelines are for reference only.

Sources:

- http://blog.hirerabbit.com/5-terrific-examples-of-company-social-media-policies/
- http://socialmediagovernance.com/policies/

5.2.1. General guidelines

- Be transparent, allow for an enjoyable atmosphere, and connect
- "Take care of the Government and yourself": Ensure that both legal and confidentiality guidelines are respected for all parties.
- Ensure that there is social media account ownership i.e. accounts should not be carelessly shared and the persons managing the accounts should be held responsible for their proper usage.
- Principles of integrity, professionalism, privacy and impartiality should be observed by social media managers/moderators when posting online.
- The authenticity of what staff post is important. Any content must be verified from credible sources before posting it. Proper copyright and reference laws should be observed when posting online.
- Dishonourable content such as racial, ethnic, sexual, religious, and physical disability slurs are not tolerated.

5.2.2. Public Brand and Usage

- When using their personal accounts, staff are allowed to associate themselves with the corresponding Ministry/department when posting but they must clearly brand their online posts as personal and purely their own. **The Government should not be held liable for any repercussions the employees' content may generate.**
- It is important for staff to properly define their association with the public body, in the same manner as they would do in the real world.

5.2.3. Staff code of conduct for Online Communications

- "Your job comes first. Unless you are an authorized Social Media Manager, don't let social media affect your job performance."
- If a staff has posted content that is potentially damaging or that contains errors, the first step should be to correct it immediately and be clear about what has been done to fix it. It is better to remain honest and publicly accept a mistake rather than try to cover up the incriminating content.

6. RECOMMENDATIONS

The setting up of a social media presence for a public body will require a number of considerations elaborated earlier, in addition to the guidelines for online communication (section 5). Thus, a checklist of important tasks/milestones is given below for an easier transition.

It is suggested that the public body consider the following tasks:

i. Identify a social media implementation team to initiate and follow up on the subsequent tasks.
It is suggested that a public official, not lower than APS, chair the meetings of this team.

ii. Elaborate on the objectives of the public body regarding the use of social media.
An example would be at the National Disaster and Risk Reduction Management Centre. The NDRRMC might use social media to share important updates on general disaster preparedness, information on workshops, work being done for disaster prevention, feedback from public (e.g. a person may raise concern on flooding in his area) and weather alerts.

iii. Ensure that these objectives are approved at upper management level. *The objectives could be discussed and approved at the level of an IT monitoring committee or a meeting with appropriate participants including the CIB and/or CISD. It is also important to ensure that confidential information is not being published carelessly, thus legal advice may be considered in some cases.*

iv. Identify which social media platforms are best suited to attain the objectives set.
Most Ministries/departments will find that using both Facebook and Twitter will be suitable for their requirements. YouTube may be considered in cases where important multimedia content can be shared with the public at regular intervals (e.g. recordings of national assembly meetings, sensitisation of public on important matters)

v. Finalise the social media team as per Table **4**.
It is specially important to identify a social media manager, who will be responsible for vetting the content of the messages being published

vi. Ensure that the appropriate infrastructure is available
The infrastructure will include computers and an Internet connection. Digital cameras or more sophisticated equipment may optionally be considered in case media content is published frequently. In case hardware requirements do not match/exceed the minimum requirements from section 3.1, the CIB may be contacted for assistance in drafting technical requirements for IT equipment and/or assistance for upgrading the Internet connection.

vii. Review technical and communication skills for the social media team
The CIB will provide assistance in identifying which technical training is required. Regarding communication skills, the services of a public relations/communications

firm or University of Mauritius or University of Technology could be considered for a tailor-made training.