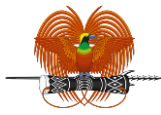


PAPUA NEW GUINEA

Department of Information and Communication Technology (DICT)

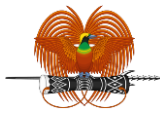
SOCIAL MEDIA STANDARDS AND GUIDELINES



DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

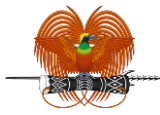
Document Control:

Document Name	Digital Government Services – Social Media Standards & Guidelines
Prepared by	PNG Digital Government Services – Department of Information and Communications Technology
Edition	Draft
Approved by	National ICT Sector Coordination Committee
Date Approved	12 th June 2021
Effective Date	
Next Review Date	



Contents

1. Introduction.....	4
2. Objectives.....	4
3. Scope.....	4
4. Intended Audience	4
5. General Recommendations	4
Recommendation 1 Understand the Risks	4
Recommendation 2 Securing Most Common Social Networking Sites	8
Recommendation 3 Proper Usage of PNG Government Crest and Agencies logos	11
6. Social Media Guidelines and Best Practices.....	15
Social Media Guidelines	16
Best practices.....	17
7. Standards for appropriate conversation	18
8. Social Media Desk	19
9. Annexure	20
Annex 1. Social Media Incident Classification and Reporting flow charts	20
Annex 2: Social Media Management Desk (SMMD) Operations.....	22
Annex 3. Social Media Account Creation Checklist	23



1. Introduction

Social media is a departments or agency's identity in the virtual world. This social identity is very much linked to its department or agency public image and needs to be protected as much in the virtual world as in the real world. The social media account if not secured may open a floodgate to compromising and maligning your agency public image.

In order to encourage and enable government agencies to make use of this dynamic medium of interaction, a Standard and Guidelines for use of social media by government agencies in Papua New Guinea has been formulated. These guidelines will enable the various agencies to create and implement their own strategy for the use of social media. The document will help them to make an informed choice about the objective, platforms, resources, etc. To meet the requirement of interaction with their varied stakeholders. This document also provides mitigation advice and security controls to help reduce threats such as unauthorized access as well as steps to follow in order to retrieve a stolen account.

2. Objectives

Provide necessary guidance to help departments or agencies manage their social media accounts securely. Aids the public on the dissemination of correct government information's.

3. Scope

All government departments and agencies including Prime Minister's Office, Ministries and Members of Parliament having social media presence.

4. Intended Audience

Super Administrator and Content Administrator or Staff authorized to manage and use the departments or agencies social media accounts.

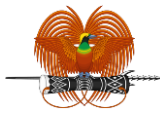
5. General Recommendations

Recommendation 1 Understand the Risks

Social media accounts related to government, semi government, national events represent an ideal and logical target for our nation's adversaries, as social media is seen as the virtual identity of the government.

Further being a government accounts, they have a huge following and the followers have implicit trust in them. The risks associated with such social media profiles are:

- Leaking of government confidential or disinformation
- Vandalism of content, misinformation



- Legal implications
- Blackmail

1.1 Set up a Governance Framework for social media

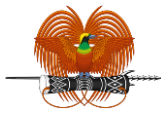
Define a policy for usage of social media in your department or agency. On a minimum, the policy should include the following:

- Identify who in the organization is authorized to engage in social media on its behalf?
- Who controls and owns the information into a social networking site?
- What information are the stakeholders passing on to other people?
- Seeking consent from stakeholder prior disseminating information related to them.
- Explicit procedures on social media networking. Who would the department or agency account follow or be influenced with etc How would information received from the follower network be broadcasted? i.e. re-shared or re-tweeted etc.
- Defined process for Incident handling / recovery plan in case of breach or malicious attacks.
- Hardware and software authorized to access the social media account from.

1.2 Account creation and administration

In order to create and manage account ownership it is recommended that we have:

- A dedicated department/agency email (usually used as the username), should be used to create and maintain a social media accounts. This email address should be a generic/nonspecific enterprise email account for logging into social media networks. Individual enterprise email addresses are easy to guess and decrease the security of social media accounts.
- Each social media channel/account should be associated with a separate and unique departments email. Example: the Username/Email associated with corporate twitter is **different from** the **Username/Email** used on Facebook
- Do not use the same passwords for social media that you use to access departments computing resources
- Private emails should not be used to manage and access a department/agency social media account such as twitter account or Facebook page



- The social media account page should feature the approved standard logo and the profile text should include references that this account is “the official” account of the department/agency.
- Government departments and agencies should define which departments / agencies they may follow. E.g., Government agencies may follow other government agencies, verified accounts or trusted sources.
- It is not recommended to follow individual users.
- It is not recommended to access / re-post / re-tweet / share “unverified messages” with imbedded links and URLs.

1.3 Account Login

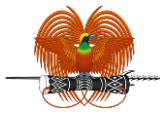
- Configure social media accounts to use secure sessions (HTTPS) whenever possible. Facebook, Twitter and others support this option.
- Login should only be from a dedicated departments owned / managed device (PC or Mobile device)
- Login should be from a trusted network, refrain from using public/open Wi-Fi networks like café’s airports...etc unless using a departments VPN to secure your session.
- If any mobile devices are linked to your departments official social media accounts, make sure that these devices are adequately protected.
- Disable the geo-location feature while posting or tweeting.

1.4 Password Management

- Always use strong and secure passwords to access social networks. The passwords should comply with the departments password policy.
- Change passwords frequently. Have different passwords for different accounts.
- Use multi-factor authentication for social media accounts (if supported by the provider).

1.5 Information Sharing / Acceptable Usage

- Do not disclose any official information upon registrations of social accounts.
- Restrict employees from posting official and sensitive data or information over social networks.
- Only authorized personnel should be allowed to operate official departments social media accounts.



- Do not post any information that may be discriminatory, disparaging, defamatory or harassing comments regarding the organization or its employees or any third party in their electronic postings or publishing.

1.6 Configure Privacy Settings

- Review and revise as necessary the default privacy settings offered by the social media networking sites.

1.7 Monitoring

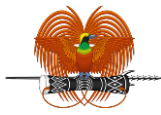
- Limit departments Official social media account access to an authorized employee in order to control the content distribution over social networks. This could be the Departments Social Media Content Administrator.
- In case where more than one person has access to the departments official social media account, internal procedures should be defined to regulate this activity, this should include training user on usage of social media, active monitoring, and use of social media management solutions and / or any other compensating controls as deemed necessary.
- Regularly monitor the access granted to authorized user accounts and revoke the access of employees who leave the organization or no longer have a business need to use social media.
- Have a third-party individual, who is not responsible for content, continuously monitor social media accounts for unauthorized or unusual postings.

1.8 Third Party Solutions

- The departments should consider usage of a social media management solution.

Incidents: In case of any suspicious activity

- Please report to DICT **Social Media Management Desk** (policy@ict.gov.pg) or call (3250148) if you see any of the suspicious symptoms below:
 - o Automated likes, favourites, follows/un-follows or friend requests
 - o Private messages being posted to your friends (this can be hard to spot unless someone points it out to you)
 - o Unexpected email/push notifications from the social network, such as:
 - o Warning that your email address has been changed
 - o Warning that your account was accessed from an unknown location.
 - o Status updates/tweets that you didn't make



- o Changes to the profile or pictures on the account.

1.9 Recovery Plan

- Collect all logs, traces, artifacts of malicious activity for investigation and possible legal requirements.
- Immediately change account passwords.
- Verify and change the password for the associated emails and back up emails
- Verify the password recovery options set for the social media account; verify the alternative email address that has been setup.
- Verify auto forward options if any setup for the account and associated emails.
- Visit the applications page of the social network and remove any apps you do not recognize. If the account continues to behave erratically, we recommend you revoke access to all applications.

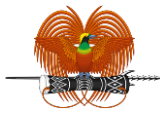
1.10 Security Awareness

- Employees managing and / or maintaining the organization's social media accounts shall be sensitized and educated on information security. They should be made aware of prevalent threats such as Phishing and social engineering.

Recommendation 2 Securing Most Common Social Networking Sites

2.1 Facebook:

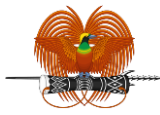
- a. Ensure you're using a secure connection whenever one is available, click Security in the left pane of Facebook's Account Settings and make sure Secure Browsing is enabled.
- b. The security settings also let you enable log-in notifications and approvals, and view and edit your recognized devices and active sessions.
- c. Security Tips:
 - i. Protect your password.
 - ii. Use Facebook's extra security features.
 - iii. Make sure your email account(s) are secure.
 - iv. Logout of Facebook when you use a computer you share with other people. If you forget, you can logout remotely.
 - v. Run anti-virus software on your computer:



- vi. Think before you click or download anything.
- d. Enable 'Login Approvals' from the 'Account Security' section of the account settings page. Follow the link - <https://www.facebook.com/notes/facebook-engineering/introducing-login-approvals/10150172618258920>
- e. Update your accounts as per new security tips and guideline of Facebook. You can find them at <https://www.facebook.com/help/379220725465972>
- f. Check also the community standards on Facebook: <https://www.facebook.com/communitystandards/?ref=cr>

2.2 Twitter:

- a. When you sign up for Twitter, you have the option to keep your Tweets public (the default account setting) or to protect your Tweets.
- b. Accounts with protected Tweets require manual approval of each and every person who may view that account's Tweets.
- c. Security Tips:
 - i. Use a strong password.
 - ii. Use login verification.
 - iii. Government departments shall get their account validated and verified. DICT Social Media Management Team can help you in this.
 - iv. Watch out for suspicious links, and always make sure you're on Twitter.com before you enter your login information.
 - v. Never give your username and password out to untrusted third parties.
- d. Using SMS text message login verification: To set up SMS text message login verification:
 - i. Go to your Security and privacy settings on twitter.com and select the option to Verify login requests.
 - ii. When prompted, click Okay, send me a message.
 - iii. If you receive our verification message, click Yes. (Note: you'll have to enter your password).
 - iv. You can generate a backup code by selecting the option to Get backup code. Write down, print, or take a screenshot of this backup code; this will help you access your account if you lose your phone or change your phone number.
- e. Update and follow the best practices mentioned by Twitter regularly. You can find them at <https://support.twitter.com/articles/76036>



2.3 Instagram:

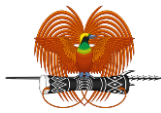
a. **Security Tips:**

- i. Pick a strong password.
 - ii. Make sure your email account is secure. Change the passwords for all of your email accounts and make sure that no two are the same.
 - iii. Logout of Instagram when you use a computer or phone you share with other people. Don't check the "Remember Me" box when logging in from a public computer.
 - iv. Think before you authorize any third-party app.
- b. Update your accounts as per new security tips and guidelines of Instagram. You can find them at <https://help.instagram.com/369001149843369>

2.4 LinkedIn:

a. **Security Tips:**

- i. Change your password regularly.
 - ii. Sign out of your account after you use a publicly shared computer.
 - iii. Manage your account information and privacy settings from the Profile and Account sections of your Privacy & Settings page.
 - iv. Keep your antivirus software up to date.
 - v. Don't put your email address, home address or phone number in your profile's Summary.
 - vi. Only connect to people you know and trust, or those you have trustworthy common connections with.
 - vii. Consider turning two-step verification on for your account.
 - viii. Be informed about reporting inappropriate content or safety concerns.
- b. Update your accounts as per new security tips and guidelines of LinkedIn, https://help.linkedin.com/app/answers/detail/a_id/267/~/-/account-security-and-privacy--best-practices



Recommendation 3 Proper Usage of PNG Government Crest and Agencies logos

If you manage an official Government social media venue on behalf of your department, provincial government, local level government, or another government administrative unit, you must use the department logo to brand the venue. You can only include the PNG Government Crest logo on your social media venue if you:

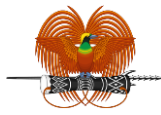
1. Are an official Government Department or Agency.
2. Represent a unit that has a presence on the e-government Portal or a department website and link back to that web presence from your social media venue.
3. Include contact information in the biography section with an email of the manager. This may be an alias email (i.e., ict.policy@ict.gov.pg).
4. Manage your social media venue in line with the standards and guidelines presented by the Department of Information & Communication Technology.

If you do not meet the criteria listed above, you cannot use the PNG Government crest and logo or any of its elements to brand your social media venue.

3.1 Facebook Pages

The timeline design of brand pages includes a cover photo that can be used by official Papua New Guinea Government Departments pages to feature our great country. Official Government Departments and Agencies Facebook pages may feature this profile picture – the golden PNG Crest symbol on a white background. Pages may differentiate themselves through their covers and through their page names. Please spell out “Papua New Guinea” within the page and include the abbreviation “(PNG)” in the name of the page or group to improve search results. *Note that only official pages may use the PNG crest symbol or any other element of the logo in their profile pictures. The use of PNG crest brand identity elements in the profile picture is not allowed for personal Facebook accounts or non-official PNG Government departments and agencies Facebook pages.

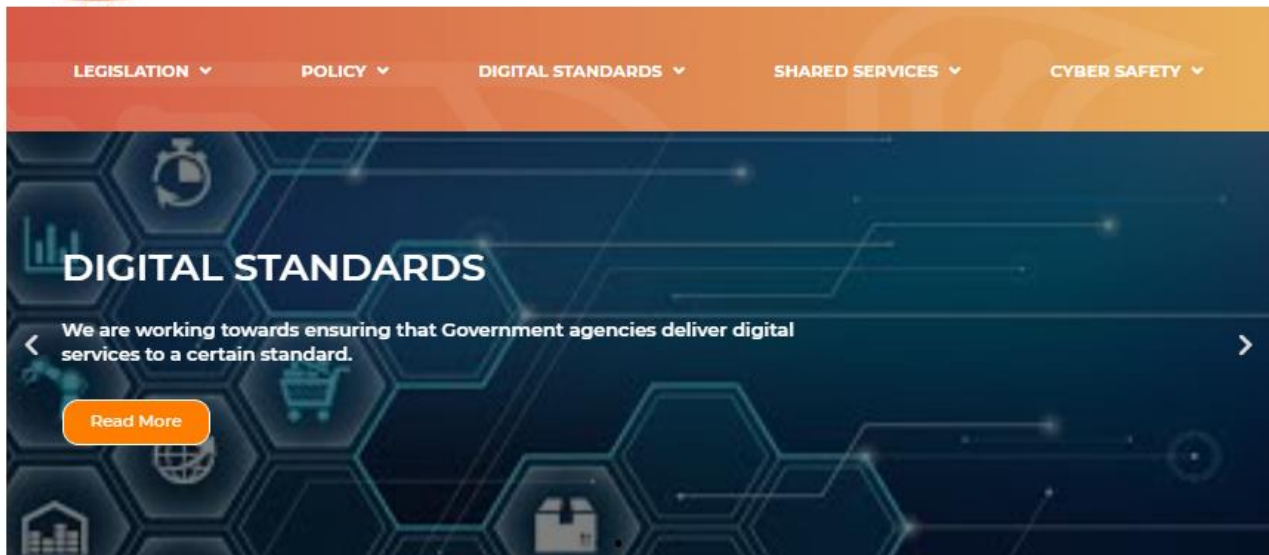
Profile Picture Format: 180 x 180 px.
The profile picture of official PNG Government Departments and Agencies Facebook pages may feature the golden symbol on a white background.



Cover Picture Format: Displays at **851 pixels wide** by **315 pixels** tall on computers and **640 pixels wide** by 360 pixels tall on smartphones.



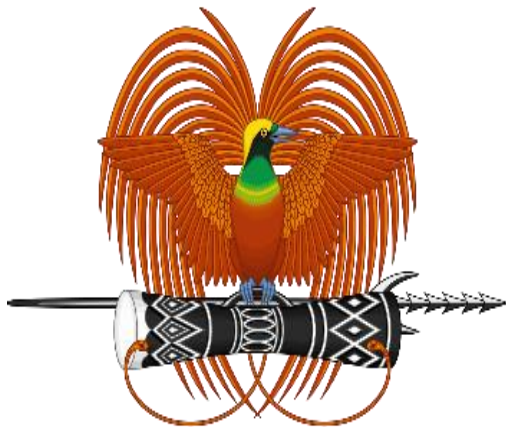
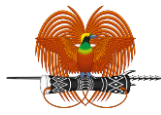
Department of Information
and Communications Technology



The cover picture provides plenty of space to feature the Government Departments and Agencies Logos, Motto, Mission and Vision Statements, as well as adding branding and unit distinction.

3.2 Instagram, Pinterest, and Tumblr

The profile picture of official PNG Government Departments and Agencies accounts on Instagram, Pinterest, and Tumblr may feature the golden PNG Crest on white background. If possible, use individual department and agency names as part of the username instead of PNG to avoid confusion with other departments and agencies using the same abbreviation. For the name of the account, include "PNG Government Department" to clearly differentiate your office or department from other Departments or agencies. Use the bio to provide a full description and include a link back to your department's website.



Department of Information
and Communications Technology

3.3 LinkedIn

The profile picture of your LinkedIn group offers very limited space to showcase the departments and agency's identity. On the other hand, the group name itself is a clearly visible distinction for the name and purposes of your group. That is why official PNG government Departments and Agencies groups on LinkedIn use profile pictures showing the centred symbol with the full Departments and Agencies name. Further unit distinction is achieved by the name of the group. Groups that are not (yet) official cannot use the PNG Crest logo or any other Departments logo as their profile picture.

Group Logo Format: Will be visible in formats up to 100 x 60 px (resized to fit)



Papua New Guinea Department of Information & Communication Technology

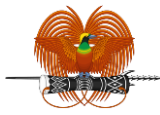
Small Logo: Will be visible in formats up to 60 x 30 px



Papua New Guinea Department of Information & Communication
Technology

3.4 Twitter

The profile picture, profile description, and the Twitter page customization, offer room for PNG Departments and Agencies identity and distinctions, whereas the Twitter



“handle” is short. Official PNG Government Departments accounts on Twitter use the profile picture and the account description to create a clearly visible identity.

SPECIAL TWITTER PROFILE REQUIREMENTS

- Include the abbreviation PNG in the “Name” field (20 characters) to improve search results.
- In the bio include the full Departments name to distinguish from other Departments that use the same abbreviation.
- Use the 160 characters of the bio to describe the account.
- Use the “Web” field in your profile to link back to your page on the departments website and include the full Departments or Agency’s name to distinguish from other Departments and Agencies that use the same abbreviation.

Profile Picture Format: 400 x 400 px width (displays 200 x 200 px)

Only the official PNG Government Department account @png on Twitter uses the profile picture with the full department or agency name. Official PNG department or agency accounts that have distinctions use the following vertical lockup, including the monogram, the symbol, and the distinction.



Department of Information
and Communications Technology

TWITTER ACCOUNT CUSTOMIZATION

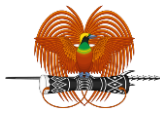
If you use any colors on your Twitter home page, make sure to use the appropriate PNG flag or crest color. If you prefer a background image, the use of an image of the department or departments activity is recommended. Make sure that you have the copyright to use the image.

IMAGE GUIDELINES

- Recommended 1,080 x 608 pixels.
- Minimum 480 x 270 pixels.
- Maximum 2,120 x 1,192 pixels.

3.5 Flinkr

For the photo-sharing site flickr, an official department or agency account for your office or department should use the golden symbol on white or green background. The name of the account should include "Papua New Guinea Department of".



Include a link back to your web pages on the Departments Website in the description. Remember to tag your photos #PNGDICT.



3.6 Youtube

YOUTUBE CHANNEL VISUAL CUSTOMIZATION

Channel avatar: 100 x 100 px squared format icon that displays next to the channel name. Official PNG Department or Agency YouTube channels use the Department or Agency logo as their avatar. In combination with a channel name that includes the full PNG Department or Agency name, the channel will be clearly branded as official and still be distinct through the unique page name.

Channel cover photo: 2,560 x 1,440 px

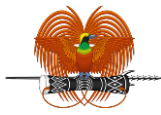
A background image showing the PNG Department/Agency or activities on departments/agencies can be used instead of a one-color background.

YOUTUBE VIDEO BRANDING

Videos produced by any Departments or agencies need to have start and/or end slide(s) that show the PNG Crest and the Departments logo.

6. Social Media Guidelines and Best Practices

These guidelines were developed for state agencies, administrators and staff of the PNG Government departments and agencies who create and administer social media sites such as Facebook, Twitter, LinkedIn, google+, Instagram, Pinterest, Tumblr or YouTube on behalf of the department or agency. DICT supports the use of social media as a valuable tool to disseminate information and create a thriving online community.



These sites reflect on the departments/agencies and should therefore be written and structured in an appropriate, ethical, professional and lawful manner. If activity on a social networking site is offensive or violates social media policy, it may result in disciplinary or legal action. Using the departments official media sites and approved accounts indicates that you have read and will abide by these guidelines.

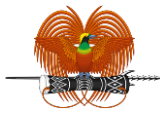
Social Media Guidelines

Guideline 1 Setting up and monitoring social media pages

1. Before setting up a social media page representing a department or the agencies, IT Manager or Social Media Officer of each department must follow the social media standards and guidelines.
2. Consider your objectives before creating a social media page. Ask yourself:
 - What do you plan to achieve with this social media? What kind of information do you want to share or receive on the page?
 - How will you measure success? What statistics will be meaningful to you? (Number of hits, event attendance, brand recognition, links, "likes," or comments.)
 - Who will be reading and commenting on your social media site? Who are you trying to engage? How will you identify them and attract them to your networks?
 - What social media networks will you be using? Who will establish the networks? Who will be administrators?
 - Who will maintain the page? How often will it be updated?
3. The page should be used only for official government department or agency-related purposes.
4. The social media page administrator responsible for posting to the social media site must regularly monitor the page. The sites will also be monitored by the DICT Social Media Management Team.
5. Personal information should not be posted on social media sites, including but not limited to: student identification numbers, employee identification numbers, NID numbers, personal addresses or phone numbers, or driver's license numbers.
6. Social media sites are not private, and the expectation of privacy is not conveyed to you as a user or administrator of the site.

Guideline 2 Photo guidelines

Photos posted on social media pages should favourably portray the departments or agencies and the persons depicted in the photos. The following guidelines should be used when posting photos:



- Photos of children should not be posted without express consent from their parents, except photos taken at public events. Even then, use great caution when posting photos of young children.
- Photos of public events can be posted on social networking sites, but they must be appropriate. As a guideline, they should be photos that could be posted on the department's official website. Examples of photos that should be avoided include but are not limited to: photos involving alcohol, nudity, medical and hospital patients, and graphic scenes.
- Photos taken on occasions that are not public, such as a workshop or class, must not be posted.

Guideline 3 Logo and titles

The name of the department/agency should begin the title of any social network page associated with a single department. For example:

- Department of Information and Communication Technology
- ICT Department

The department or agency logo cannot be used on Facebook pages except on the official department/agency page.

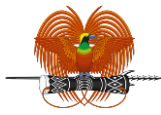
Guideline 4 Administration

At least two site administrators (Super Admin & Content Admin) are recommended. For outgoing and incoming administrators should be overlapped to ensure a smooth transition.

Best practices

Freedom of speech must be exercised responsibly on the sites. These recommendations provide a roadmap for constructive, respectful, and productive use of social networking sites.

- **Be respectful**
Respect your audience and your colleagues. Take care not to engage in any conduct that would not be acceptable in the workplace.
- **Get your facts straight**
Ensure that you are providing accurate information so that you are not misrepresenting the departments or the agencies.
- **Be mindful of your public image**
Consider the image you want to portray to the public. Be mindful that what you



post may be viewed by the international community, PNG Citizens, students, administrators and community members, and may stay public for a long time.

- **Use your best judgment**

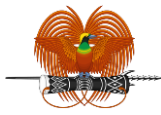
Remember there may be consequences to what you post, so consider your content carefully. If you are about to post something that makes you the slightest bit uncomfortable, review these guidelines and think about whether to post the material.

7. Standards for appropriate conversation

Although online conversations on social media sites are often casual, they must remain professional and respectful. Comments on the Government **Departments, Prime Minister's Office, Ministers Office** and **Members of Parliament** official pages are monitored to ensure compliance with the social networking standards and guidelines. Inappropriate comments or posts and fake accounts will be removed by the Social Media Management Desk.

Content, individual account and page that will be deleted includes:

- Misinformation
- Disinformation
- Threat to the Prime Minister, Minister or a Member of Parliament
- An advertisement for a commercial business
- Libellous, slanderous, inflammatory or defamatory comments
- Vulgar, racist or sexist slurs
- Obscenities
- Comments pertaining to violence
- Information that violates citizens privacy
- Comments that are not respectful.
- Comments that are not relevant to the topic.
- A commenter who is misrepresenting himself/herself.



- A single person who is dominating the conversation.
- Individual or group account that post misinformation
- Political Groups that post misleading information

8. Social Media Desk

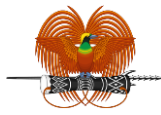
The **Social Media Management Desk** have the authority under the **NEC Decision 100/2021** to Monitor, analyze and control the information dissemination. Any content that is posted by any individual or a page that contains or comes under the two categories such as;

I. Misinformation

II. Disinformation,

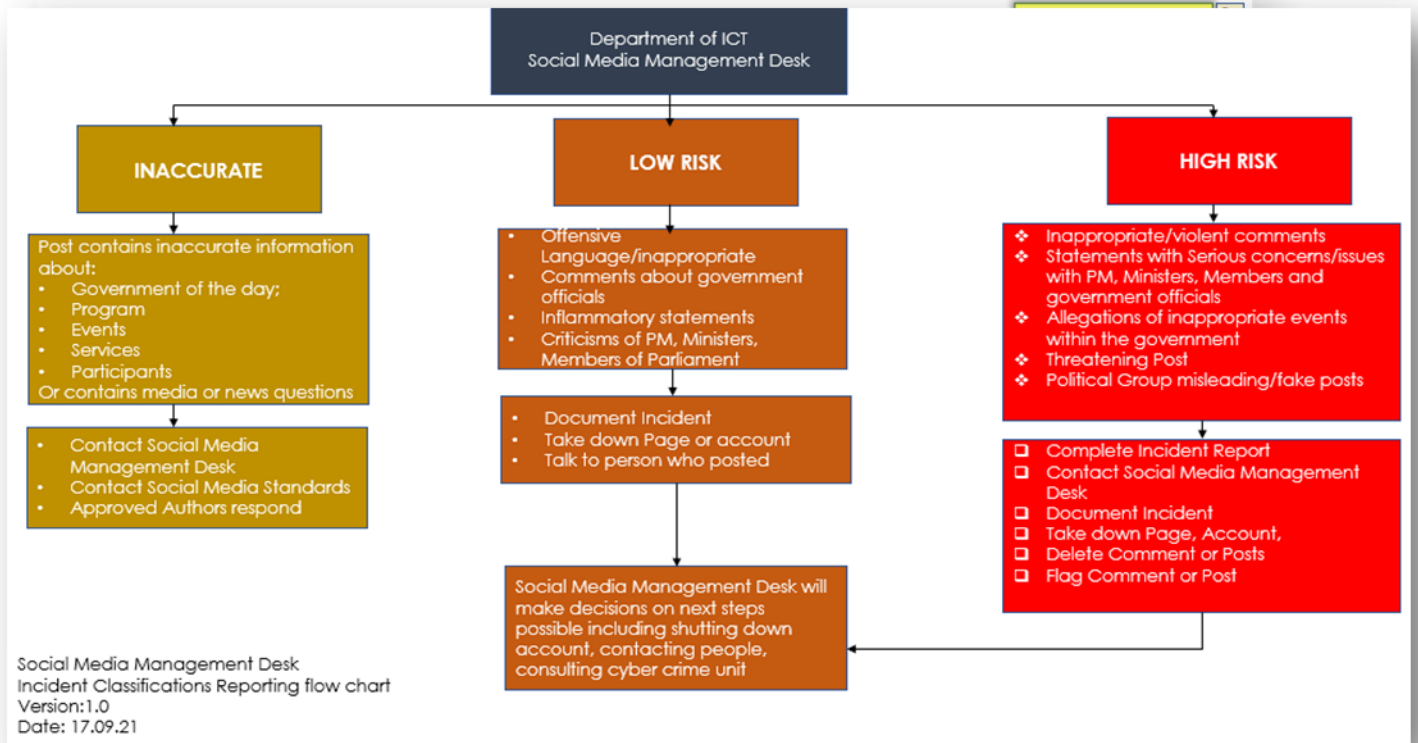
will be taken down or deleted within the next 24 hours. The person responsible will be dealt with accordingly under the cybercrime act.

This also applies to the fake account holders impersonating the **Prime Minister, Ministers, Members of Parliament and Government Agencies.**

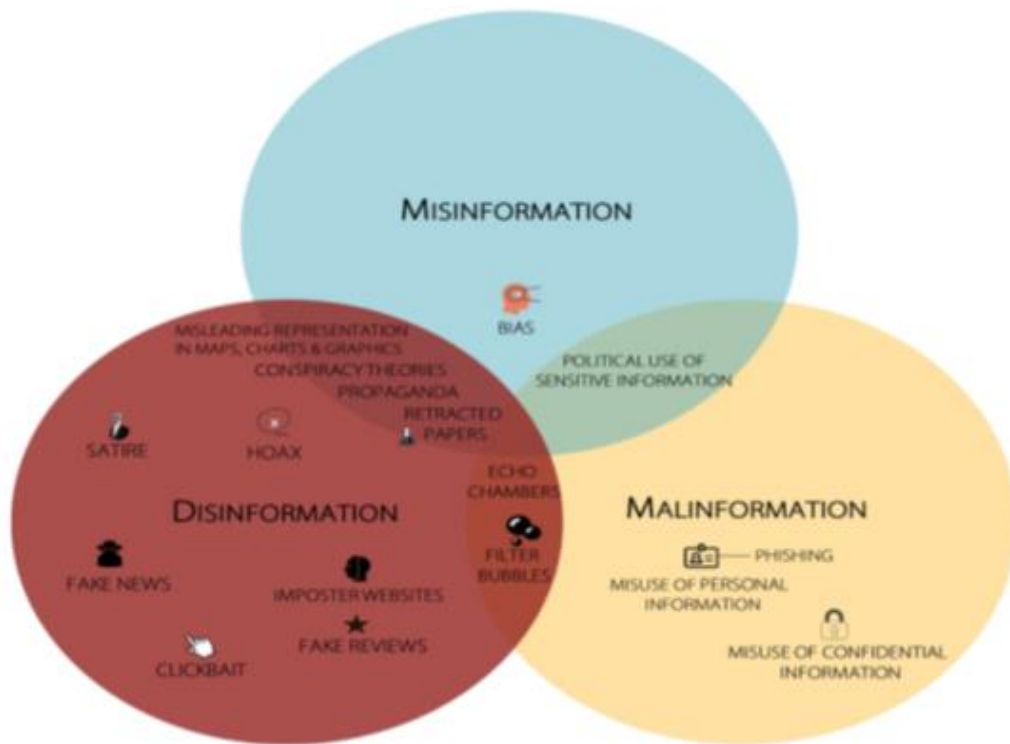
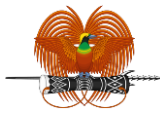


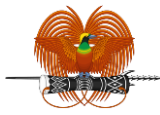
9. Annexure

Annex 1. Social Media Incident Classification and Reporting flow charts

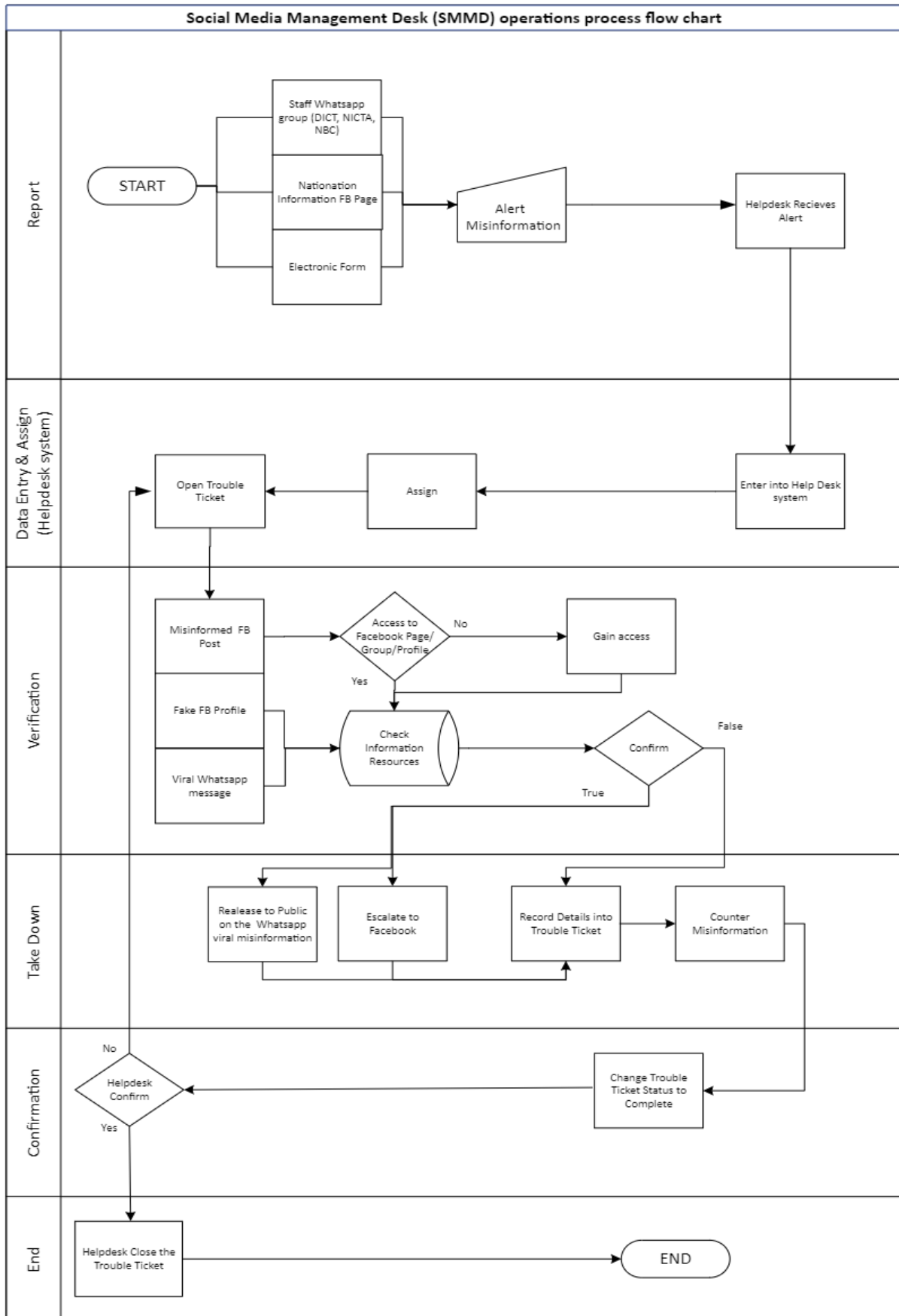


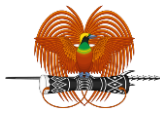
Social Media Management Desk
Incident Classifications Reporting flow chart
Version:1.0
Date: 17.09.21





Annex 2: Social Media Management Desk





Annex 3. Social Media Account Creation Checklist

PNG Government Departments and Agencies Social Media Standards and Guidelines Checklist

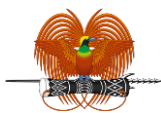
Departments Name :
.....

Social Media Address :
.....

Use of social media technologies must follow the current laws and standards that govern information and information technology. Below is a list of the most common standards and policies that apply to the use of social media. Visit <https://www.ict.gov.pg/web> for more information and contact vanessa.panap@ict.gov.pg if you have questions.

The checklist should be considered alongside agency-specific guidelines and policies governing social media use in your workplace.

Section	Checklist	Tick where appropriate	
		YES	NO
1	Departments/Agency's Name		
2	Department Logo/PNG Crest is applied to; An official Government Department or Agency		
3	Two or more Super Admin and Content Admin		
4	Represent a unit that has a presence on the e-government Portal or a department website and link back to that web presence from your social media venue		
5	Include contact information in the biography section with an email of the manager. This may be an alias email (i.e..policy@ict.gov.pg).		
6	Determine process to moderate (review and clear) comments. Clearly link to a comment policy if you will allow comments		
7	NO third-party website used as link to official social media account		



DEPARTMENT OF INFORMATION AND COMMUNICATION TECHNOLOGY

8	Have you obtained the consent of others before posting their personal information?		
9	Make sure you have received permission to use any trademarked images and logos.		
10	Post approvers or Admin must be up to date with the post and be genuine and precise on the posters and the postings.		

Comments:

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

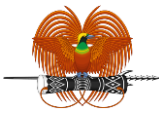
.....

.....

.....

.....

Compiled By	
Division/Wing	
Position	
Date	
Signature	



PNG Digital Government Services – Managers Recommendations (Digital Wing)

.....

Name	
Position	
Division/Wing	
Date	
Signature	