PAPUA NEW GUINEA

Department of Information and Communications Technology(DICT)

Government Social Media Standards and Guidelines 2025

Document Control:

Document Name	PNG Government Social Media Standards Guidelines 2025
Prepared by	PNG Digital Government Services–Department of Information and Communications Technology
Edition	Draft 2
Approved by	National ICT Sector Coordination Committee
Date Approved	
Effective Date	
Next Review Date	

Table of Contents

Government Social Media Standards and Guidelines 2025

PART I.-PRELIMINARY

1.Name

This instrument is the Government Social Media Standards and Guidelines 2023.

2.Commencement

This instrument commences on [1 July 2024].

3.Authority

(1) This instrument is made under Section 64 of the Digital Government Act 2022.

(2) This instrument is also made under Section 41 of the Digital Government Act 2022.

(3) This instrument has been produced by the Department of Information and Communications Technology(DICT).

4.Simplified Outline

(1) This instrument prescribes standards and guidelines for government social media accounts.

(2) Part 1 sets out preliminary matters.

(3) Parts 2 sets out Standard 1, Standard 2 and Standard 3. Part 2 contains mandatory standards.

(5) Part 3 contains Social Media Guidelines and Best Practices. Part 4 contains other relevant matters together with Appendix 1.

(6) Notes are included in this instrument to help understanding by drawing attention to other provisions information or explanations. The notes are in small type, so that they don't disrupt the text. They do not contain statements of law.

5.Definitions

In this instrument, unless the context otherwise requires-

"Accessibility "in the context of social media means making content and digital assets usable by individuals with disabilities. This includes providing alternatives like alt text, captions, and screen reader compatibility.

"Analytics" in the context of social media involves collecting and analyzing data related to social media performance, including metrics such as engagement, reach, impressions, and follower growth.

"Algorithm" means a set of rules or calculations used by social media platforms to determine the order and visibility of content in users' feeds.

“Content Calendar” means a schedule that outlines when and what content will be posted on social media, helping organizations plan and organize their messaging.

“Crisis Communication” means the process of managing and responding to sudden, unexpected events or situations that can negatively impact an organization's reputation or operations, often through social media channels.

“Employee Advocacy” means a strategy where employees actively promote and represent their organization on social media by sharing company content, participating in discussions, and advocating for their mission and values.

“Engagement” means engagement on social media measures the interactions between an organization's content and its audience, including likes, shares, comments, and clicks.

“Geotagging” involves attaching location data to social media posts, indicating where the content was created or where an event occurred.

“Hashtag” means a word or phrase preceded by the “#” symbol used to categorize and index content on social media. It helps users discover and follow specific topics or trends.

“Impressions” means the total number of times a piece of content is displayed on users’ screens, regardless of whether it was clicked or engaged with.

“Official Social Media Account” means an official social media account is a social media profile or page that is owned, managed, and authorized by the organization for official communication and representation.

“Moderation” means monitoring and managing user-generated content on social media to ensure it complies with community guidelines and policies. This may include removing or hiding inappropriate or harmful content.

“Privacy Settings” means the configurable options that allow users to control the visibility of their personal information and posts on social media platforms, determining who can access their content.

“Social Listening” means monitoring social media platforms to track and analyze conversations, mentions, and trends related to an organization, industry, or specific keywords.

“Social Media” means a digital platform and website that allow users to create, share, and interact with content and other users. Common social media platforms include Facebook, Twitter, Instagram, LinkedIn, and YouTube.

“Third-Party Solutions” means products, services, directories, networks, applications, software, and other materials that may be used.

“Trolling” means the act of deliberately posting inflammatory, offensive, or disruptive comments or content on social media to provoke reactions or disrupt discussions.

“User-generated Content” (UGC)means content created and shared by individuals who are not part of the organization, such as comments, reviews, and posts made by the public on the organization's social media accounts.

6.Objectives of Standards and Guidelines

- provide the necessary guidance to assist public bodies to manage social media accounts securely;
- provide a uniform and consistent mode of communication across all social media platforms;
- facilitates a safe and responsible engagement between followers and government social media accounts.
- aids the host government body on the dissemination of accurate information;
- encourages engagement and discussion between the host government and the public bodies and the public

7.Scope and Application

(1) The following applies to;

- all social media accounts created by any public body.
- Super administrators and content administrators will manage government social media accounts.

(3) An entity that is not a public body but chooses to follow this instrument.

PART II.-GENERAL STANDARDS

Standard 1: Social Media Account Management

8.Overview

(1) Social media accounts related to the government are an ideal and logical target for our country's adversaries as social media is viewed as a virtual identity.

(2) With the increase in use of technology, social media platforms have fast become a preferential channel of communication and means of interaction between the government and the public.

(3) Growing use of social media by public bodies also presents cyber challenges and risks, such as;

i. Leaking of government confidential information
ii. Misinformation or disinformation
iii. Vandalism of content
iv. Blackmail
v. Cyber attacks
vi. and other associated risks.

(4) This instrument establishes a foundation for understanding social media and managing government accounts.

(5) These standards are mandatory.

Standard 1.1 Set up a governance framework for social media accounts

(1) All public bodies must comply with existing policy and legislative frameworks before the setup, usage, and management of social media accounts.

(2) Policy and legislative frameworks include;

- Identification of super administrators and content administrators.
- Establishing controls and ownership of the information on the social networking sites.
- Determination of information the stakeholders share to other people.
- Process of getting a stakeholder's permission before sharing 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 broadcast?i.e.re-shared or re-tweeted etc.
- Defined processes for Incident handling or recovery plan in case of a breach or malicious attacks.
- Recommended and authorized hardware and software for accessing social media accounts.

(3) The table below further outlines what should be included in all social media governance frameworks.

Key component	**Details**
Social media management	i. Social media management covers all areas concerning social media, this includes; a. which social networking sites are used, b. account administration and access, c. how content is published, d. social media strategies, e. engagement with followers and monitoring and training procedures. ii. This also includes social media security.
Social media strategy	i. The social media strategy includes; a. policies b. procedures, c. and guidelines. ii. Each account could have different goals,however,through a good social media strategy it helps to stay in synchronization with the overall department/agency’s objectives and core functions.
Security	Security includes; a. password policies b. data privacy, process of reviewing accountant c. security settings.
Crisis Management	Crisis management in social media describes the best way to use social media in an emergency or crisis.

Monitoring and reviewing	This includes; a. monitoring b. reviewing and c. compliance tests of the social media account.
Training	Training strategies for all employees or social media account administrators.

Figure 1 Key components of social media governance framework

Standard 1.2 Account creation and administration

In the creation and administration of a government social media account, the following applies:

i. The public body must have at least a social media presence on one or more social networking sites.

ii. Each public body will determine which social networking site to use basing on organizational goals, needs, and resources.

iii. An official department/agency email should be used to create and maintain social media accounts.

iv. Each social media channel/account must have a separate and unique departments email. For example, the username/email associated with corporate twitter is **different from the Username/Email** used on Facebook.

v. Each social media account must have its own password if the department/agency administers multiple social media accounts.

vi. Private emails should not be used to manage and access government social media accounts.

vii. Approved standard logo must be used for all social media accounts.

viii. Follow only verified accounts, or trustworthy sources.

ix. It is not recommended to follow unofficial accounts of government officials, especially elected officials and heads of government bodies.

x. Public bodies must not access/re-post/re-tweet/share" unverified messages" with imbedded links and URLs.

Standard 1.3 Account Access and Logins

When accessing social networking sites;

i. Configure government social media accounts to use secure sessions(HTTPS). This option is supported by Facebook, Twitter, and others.

ii. Access social media accounts from a dedicated department owned/managed device (PC, laptop, or smartphone). These devices must be installed with the latest updated endpoint protection (refer to Standard 2.2).

iii. The login must come from a government-approved network. Use public/open Wi-Fi networks like cafés, hotels, and airports ONLY if they are connected through a trusted VPN to secure the session.

iv. Ensure that these devices are adequately protected if the account is linked to a mobile device

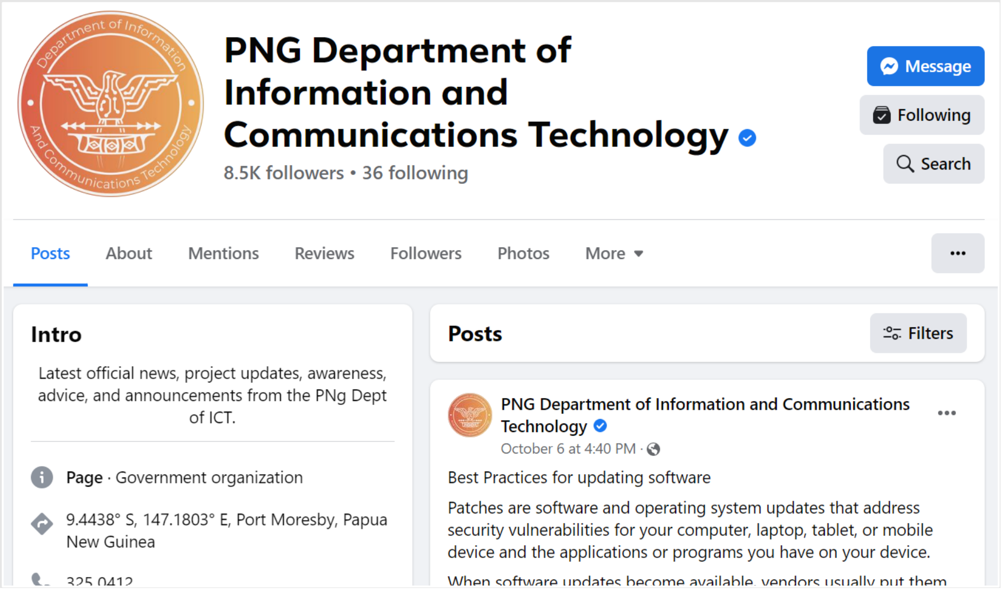
v. Disable the device geo-location feature while posting or tweeting, for security purposes.

vi. Document authorized staff for administration and content upload that access all government social media accounts.

Standard 1.4 Account verification

(1) Official government social media accounts must be verified. This builds the trust between the followers and the government entity.

(2) Social media verification can greatly benefit the government entity' social media presence. The blue tick/check verifies that the account is real and genuine account.



PNG Department of Information and Communications Technology ✓

8.5K followers • 36 following

Latest official news, project updates, awareness, advice, and announcements from the PNg Dept of ICT.

Page · Government organization

9.4438° S, 147.1803° E, Port Moresby, Papua New Guinea

325 0412

PNG Department of Information and Communications Technology ✓

October 6 at 4:40 PM ·

Best Practices for updating software

Patches are software and operating system updates that address security vulnerabilities for your computer, laptop, tablet, or mobile device and the applications or programs you have on your device.

When software updates become available, vendors usually put them

Figure 2 Snippet of verified DICT Facebook Account

(3) The above Figure shows a screenshot of DICTs Facebook account which shows the blue tick beside its name. This shows the public that this is the official government social media account. All government entities should consider getting social media accounts verified.

Standard 1.5 Password Management

(1) For all government social media accounts, strong passwords are recommended.

(2) Passwords must have at most 8 characters, at least one being a capital letter, one numeral and one symbol.

(3) Each social networking site must have different passwords, and these passwords must be changed frequently for security purposes.

(4) Multi-factor authentication should also be used for optimal social media security.

Standard 1.6 Information Sharing/Acceptable Usage

(1)All government social media accounts must consider the following;

i. Do not disclose any official information upon registration of social accounts, unless authorized.
i. Employees must not post official, sensitive or confidential data or information over personal social media accounts.
ii. Only administrators are allowed to operate government social media accounts.
iii. Administrators must not post any content that is considered discriminatory, disparaging and defamatory, or harassing comments regarding the public body, its employees or any third party.

Standard 1.7 Monitoring All Social Media Activities

All administrators must consider the following;

i. Limit government social media account access to an authorized employee to control the content distribution over social networks. This could be the Content Administrator.
ii. In the 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.
iii. 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.
iv. Continuous track comment mentions. These are instances that the name of government entity is mentioned in a comment, or post.
v. It is also recommended to assign persons without administrative control to continuously monitor social media accounts for unauthorized or unusual postings.

Standard 1.8 Third-Party Solutions

(1) All public bodies must consider utilizing recognized third-party solutions to use in content creation as well as management.

(2) Public bodies must consider using approved open-source or software that requires payment plans.

(3) All incidents or suspicious activities must be reported to the Social Media Management Desk(SMMD)of the Department of Information and Communications Technology immediately.

(4) Common suspicious symptoms are as follows;

i. Automated likes, favorites, follows/un-follows or friend requests.
ii. Private messages being posted to your friends (this can be hard to spot unless someone points it out to you)
iii. Unexpected email/push notifications from the social network, such as:
  - Warning that your email address has been changed
  - Warning that your account was accessed from an unknown location.
  - Status updates/tweets that you didn't make
  - Changes to the profile or pictures on the account.

(5) Figure 2 recommended Social Media management tools that can be utilized by admin users to control and monitor the social media activities.

Management Tools	Features/Capabilities includes;
MELTWATER	• track and analyze social media content • media monitoring • outreach, and social listening •
DETERM	• Online monitoring tool that gives marketers control over brand, product, or service mentions instantly and in any language. • It's especially helpful for managing brands' reputations online and dealing with any unexpected crises.
AGORAPULSE	• With Agora pulse, you can keep all of your marketing activities organized. • complete, all-in-one solution combining social media management and monitoring features,so,it's no surprise that many well-known companies effectively use this tool.
HOOTSUITE	• Hoot suite covers almost every aspect of marketers' work, helping them to manage organic and paid social media content, measure performance, as well as share and schedule social media posts. • Using this tool properly can quickly increase a team's productivity.However,how does it work as a social media monitoring solution?

BRANDWATCH	• social media analytics tool focused more on the needs of large companies than those of smaller businesses. • The tool appeals more to those looking for a data-driven interface than one that is visually appealing.
MENTION	• Mention is a tool that combines social media monitoring features with listening solutions. • It’s a powerful tool for tracking mentions, but many companies use it mainly as a social media management tool.
SENDIBLE	• social media management platform designed for agencies looking to manage social media more effectively. • It does not focus on monitoring social media but rather on planning,scheduling,and facilitating team collaboration.

(6) The tool should be verified and approved by the Department of Information and Communications Technology before it is used by a public body.

Standard 1.9 Conduct internal social media audits

(1) Public bodies must conduct internal social media audits to assess growth, opportunities, and what can be done to improve your social presence using key social media metrics.

(2) Five basic social media reviews must be undertaken:

i. Performance reviews
ii. Content performance review
iii. Audience demographics
iv. Workflow reviews
v. Social media goals alignment

Standard 1.10 Social media training

All public bodies must provide proper social media training and short courses to all administrators and other staff to properly monitor government social media accounts.

Standard 2 Social Networking Sites Security

9.Overview

(1) For optimal social media security, the following standards act as a guide. These are highly recommended standards that all public bodies must follow to make sure social accounts are secure.

(2) According to Fortinet, the most common social media-related cyber threats to be aware of are as follows:

- Social Engineering
- Phishing
- Malware
- Brand impressions

- Catfishing

Standard 2.1 Passwords policies for government social media accounts.

(1) All government entities must:

i) Ensure strong and secure passwords.
ii) comply with relevant password policies, both internal as well as social networks.
iii) Use of complex and unique passwords.
iv) Avoid using keywords like the name of the account, for example, name of government entity in the password.
v) Regularly change passwords.
vi) ensure only administrators have access to accounts.

Standard 2.2 Protect all endpoints

(1) Social networking sites can now be accessed from multiple endpoints, including laptops, tablets, and smartphones.

(2) Public bodies must ensure all endpoints have the right endpoint protection solutions for each device.

(3) For endpoint protection, refer to Digital Government Cybersecurity Standards and Guidelines 2023 for further information.

Standard 2.3 Configure Privacy Settings

(1) Public bodies must review and revise the necessary default privacy settings offered by the social networking sites.

(2) For specifications, refer to the Digital Government Cybersecurity Standards and Guidelines 2023.

Standard 2.4 Update security settings across all sites

(1) Public bodies must not rely solely on the default settings of a social networking site, especially security settings and privacy settings.

(2) Public bodies must adjust these settings manually to ensure the highest level of protection for your social media accounts.

(3) Public bodies must always check and update these settings regularly, go through your applications and platforms and delete any that is no longer in use.

Standard 2.5 Update of applications

(1) Public bodies must regularly update applications that are used to access government social media accounts to make sure it is secure from any new threats or vulnerabilities.

(2) Refer to Digital Government Cybersecurity Standards and Guidelines 2023 for further information.

Standard 2.6 Develop recovery plans

(1) Public bodies must have an internal recovery plan.

(2) Public bodies must have detailed recovery procedures in place that help them in emergencies and other incidents.

(3) The following processes must be included in this plan:

i. Collect all logs, traces, artifacts of malicious activity for investigation and possible legal requirements.
ii. Immediately change account passwords.
iii. Verify and change the password for the associated emails and back up emails
iv. Verify the password recovery options set for the social media account; verify the alternative email address that has been setup.
v. Verify auto forward options if any setup for the account and associated emails.
vi. 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.

(4) Refer to Digital Government Cybersecurity Standards and Guidelines 2023 for further information.

Standard 2.7 Security Awareness

(1) Public bodies must ensure administrators managing and/or maintaining the government social media accounts must be regularly sensitized and educated on information security.

(2) Public bodies must have an internal training plan.

Standard 3 Usage of PNG Government Crest and Logos

10.Overview

(1) The official department/agency logo must be used to brand any official government social media account that you operate on behalf of any public body.

(2) The PNG Government Crest logo must be used on social media accounts only if the public body:

(a)Is an official Government Department or Agency.

(b)Represents a unit that has a presence on the e-government Portal or is related to a public body.

(c)Provides contact information for designated social media administrators for inquiries and reporting issues.

Standard 3.1 Usage on Facebook, Instagram and Pinterest accounts

(1) Official government Facebook pages must use the PNG crest and or official logo.

(2) The design of home pages must include a cover photo

PNG Crest symbol on a white background-must appear on official government departments and agencies' Facebook pages.

(3) The cover photo must feature Government Departments and Agencies Logos, Motto, Mission and Vision Statements.

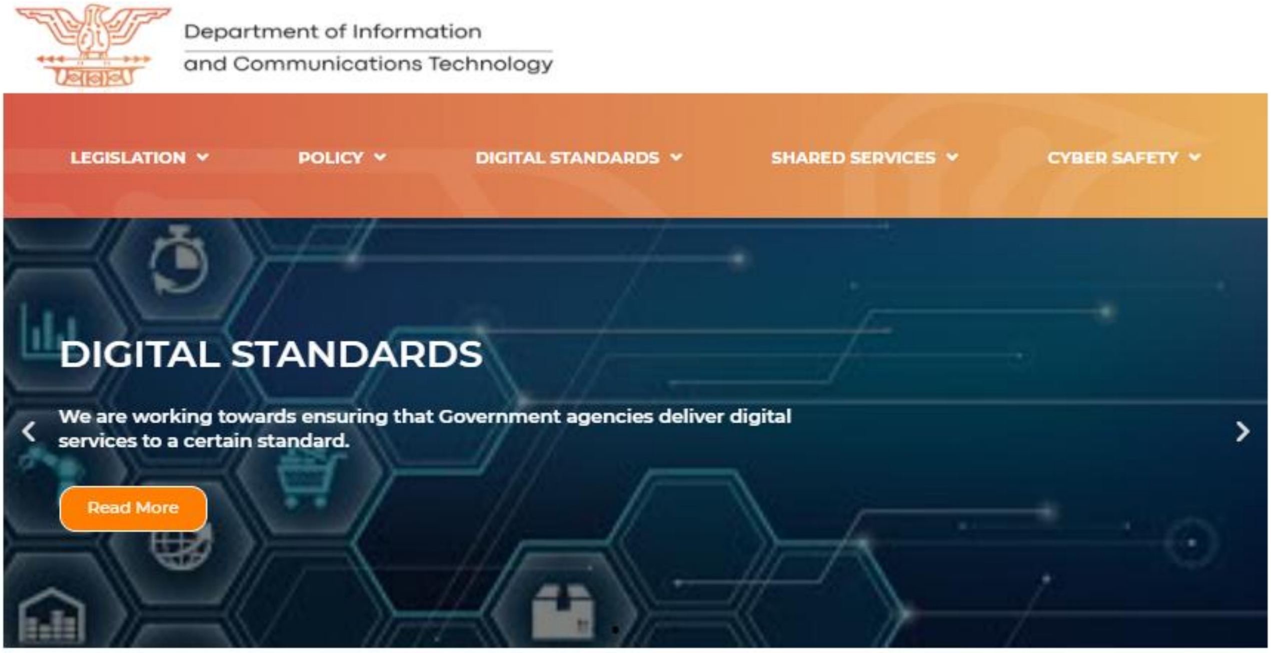
(4) Social media pages must be distinguished by the department/agency name in full.

(5) Personal Facebook accounts or entities that are not public bodies must not use PNG crest.

Profile Picture Format:180 x 180 px

Papua New Guinea

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



DIGITAL STANDARDS

We are working towards ensuring that Government agencies deliver digital services to a certain standard.

(6) Public bodies must use the bio section to give an explanation and to link to the department/agency's website.

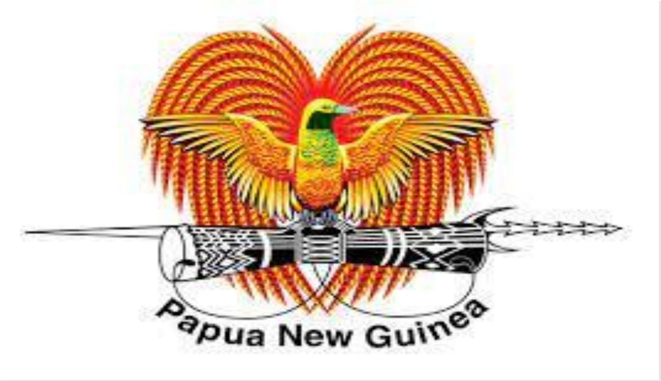
Standard 3.2 Usage on LinkedIn

(1) The LinkedIn profile picture provides very little space to showcase the departments’ and agency's identity.

That is why official PNG government Departments and Agencies groups on LinkedIn use profile pictures with the centered symbol and the full name of the Departments and Agencies.

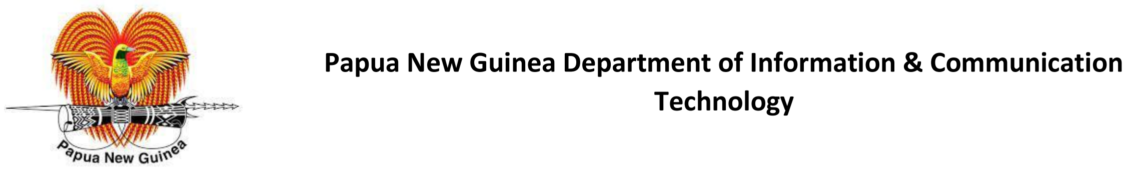
(2) Non-official groups must not use the PNG Crest logo or any other Department's logo as their profile picture.

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
Papua New Guinea Department of Information & Communication Technology

Standard 3.4 Usage on Twitter

(1) The profile picture, profile description, and Twitter page customization allow PNG Departments and Agencies to express their identity and distinguish themselves, whereas the Twitter"handle"is short. Official PNG Government Department Twitter accounts use the profile picture and account description to create a clear and distinct 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)

(2) The profile picture with the full department or agency name is only used by the official PNG Government Department account@png on Twitter. Official PNG department or agency accounts with distinctions use the vertical lockup shown below, which includes the monogram, symbol, and distinction.

Department of Information
and Communications Technology

TWITTER ACCOUNT CUSTOMIZATION

(3) Use the appropriate PNG flag or crest color when colors are used on Twitter home pages. If background images are preferred, an image of the department or its activities is recommended. Check that right image are also used.

IMAGE GUIDELINES

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

Standard 3.5 Usage on 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 must show the PNG Crest and the Departments logo.

Part III.-SOCIAL MEDIA GUIDELINES AND BEST PRACTICES

11.Overview

(1) Social media platforms act as a valuable tool to disseminate information, provide a huge insight and project a positive public image to their target audience.

(2) Each post, comment and interaction must be written and structured in an appropriate, ethical, professional, and legal manner.

(3) These guidelines have been developed to act as a guide to the use of all government accounts operated and managed by a public body.

12.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, administrators, or social media officer of each department must follow the social media standards and guidelines.

2.Consider these objectives and questions before creating a social media page.

- What does the government entity plan to achieve with this social media? What kind of information is going to be shared or received on the page?
- How will government entity measure success? What statistics will be meaningful to the government entity? (Number of hits, event attendance, brand recognition, links,"likes,"or comments.)

- Who will be reading and commenting on the social media site? Who is the government entity trying to engage? What will be used to identify them and attract them to your networks?
- What social media networks will the government entity 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 Social Media Desk of the Department of Information and Communications Technology

5.Personal information should not be posted on social media sites, including but not limited to: student identification numbers, employee identification numbers, ID 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 Keep updated with latest news of cyber threats relating to social network sites

Always be aware of new cyber risks and threats relating to social media. This ensures administrators are aware of what is happening around the world and, these threats and risks can be closely monitored by social media teams.

Guideline 3 Administration of social accounts

(1) Two site administrators (Super Administrator Content Administrator) are recommended.

(2) Outgoing and incoming administrators must be overlapped to ensure a smooth transition.

Guideline 4 Public servants Use and Management of Personal Social Media Accounts

(1) The (Information, Social Media Management Desk or The Media team) must and will only be the right agent in any Department to disseminate any confidential information regarding the organization's movement through their authorized pages or accounts.

(2) All administrators must have endpoint devices (Antivirus Software) installed per their personal computer and other devices.

(3) Refer to Government Cybersecurity Standards and Guidelines 2023.

Guideline 5 Use of social media during emergency/crisis

(1) During disasters, emergencies, or crises, public bodies can use social media to communicate with the public to reduce the spread of misinformation.

Guideline 6 Always maintain transparency with viewers

1. Public bodies must ensure authenticity and transparency on social media accounts.
2. Public bodies must ensure correct and accurate information is published at all times.

Guideline 7 Regularly update sites with latest news, projects, and other information

(1) Public bodies must maintain a constant flow of information and regularly update its activities. Public bodies must make announcements on their social media accounts.

Guideline 8 Usage of images and other relevant media

(1) Public bodies must ensure photos, videos, and other graphics posted on social media pages portray the departments or agencies and accurate persons depicted.

(2) The following guidelines must be considered;

- Images containing minors and children under the age of 18 must not be posted without consent from their parents or guardians, except images taken at government events.
- Images of public events can be posted on social networking sites but must be appropriate.
- Examples of images that must be avoided include but are not limited to images depicting alcohol, nudity, medical and hospital patients, and graphic scenes.

Guideline 8 Logos and titles

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

13.Social Media Best Practices

Speech and Language

(1) Official government social media accounts must use appropriate and user-friendly language, comment or conversation held or posted using a government social account must consider all these following best practices:

i) **Be respectful**
Get your facts straight

ii) **Be mindful of Government public image**
Use your best judgment

Security

(1) As highlighted in Standard 2(see page 11), Public bodies must consider security implications when interacting with any individual account, page, or groups.

(2) To ensure best practices the following must be considered;

i. Enable multi-factor authentication(MFA). MFA adds an extra layer of security to your key accounts and includes biometrics, security keys, etc. That send you one-time, unique codes when you log in to a sensitive account.
ii. Do not re-use old passwords
iii. Do not use passwords that are considered "weak".
iv. Always monitor comments, posts, or other accounts
v. Always keep devices clean by updating regularly. Note that you can adjust settings to automatically send notifications for new updates.
vi. Use secure connections when accessing these government social media accounts. Do not always public WIFI's, always connect to a secure VPN.

Crisis Management

i. The following emergency best practices are derived from ISO 22329:2021;
   - Stop the spread of false information and fake news.
   - Allow viewers to engage and ask questions about a current crisis/emergency.
   - Maintain social responsibilities
   - Provide continuous real-time updates to avoid confusion.
   - Provide support, engagement and monitoring of all posts, comments and conversations happening.

14.Standards for appropriate conversation

1)Online conversations on social media sites must be casual.

2)conversations held on government social accounts must remain professional and respectful.

3)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.

4.)Inappropriate comments or posts and fake accounts will be removed by the Social Media Management Desk of the Department of Information and Communications Technology

5)Content, individual account and pages that will be removed if it includes the following:

- Misinformation
- Disinformation
- Cyber threats to the Prime Minister, Minister, or a Member of Parliament

- An advertisement for a commercial business
- Slanderous or defamatory comments
- Vulgar, racist or sexist slurs
- Obscenities
- Comments pertaining to violence
- Information that violates citizen’s 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

Part IV.-MISCELLANEOUS

15.Social Media Desk

(1) The Social Media Management Desk has 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;

(a) Misinformation
(b) Disinformation

(2) Any content that is regarded as will be taken down within 5 hours.

(3) The person responsible will be dealt with accordingly under the Cybercrime Act 2020 and other appropriate laws.

16.Monitoring and Evaluation

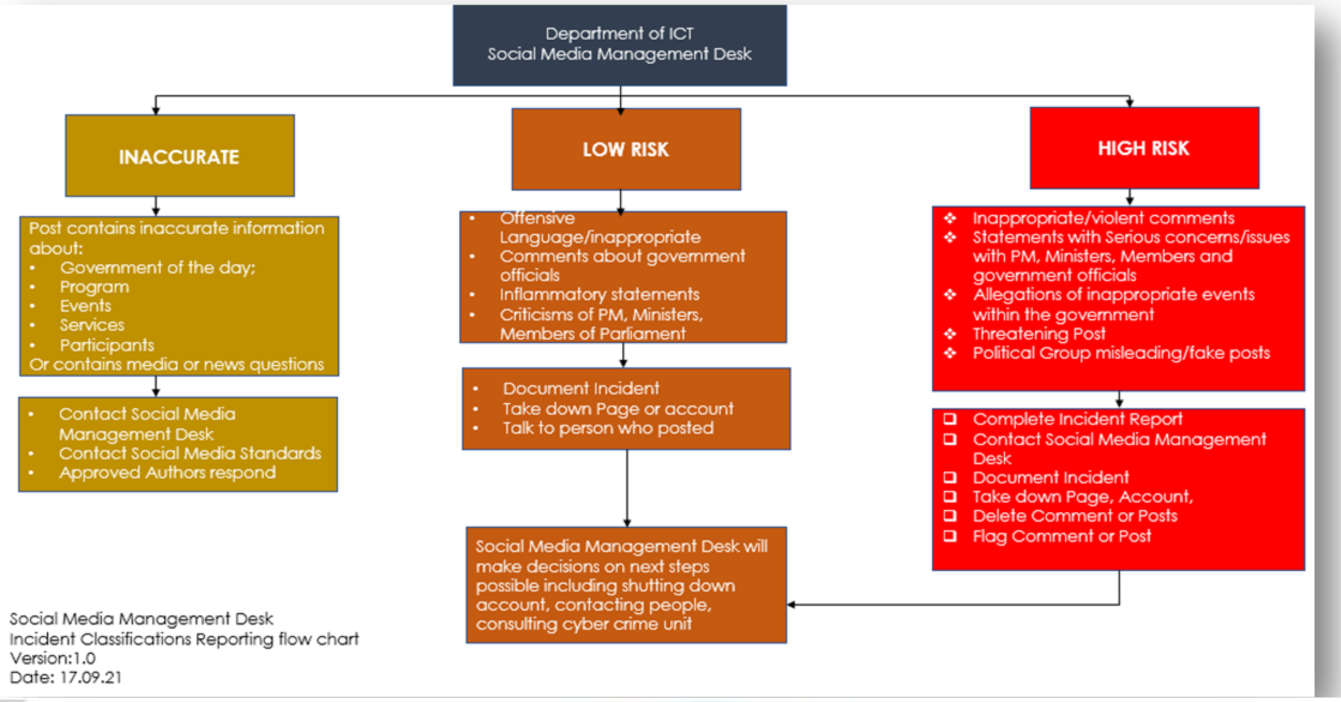
(1) All government departments and agencies should have a social media presence on the most common social networking sites such as Facebook, Instagram, Twitter, LinkedIn, or YouTube.

(2) Reviews and compliance audits be carried out to monitor and evaluate social accounts of all government entities.

(3) Audits and reviews must ensure compliance with the following prescribed standards and guidelines outlined in this document.

APPENDICES

Annex 1. Social Media Incident Classification and Reporting flow charts



Department of ICT
Social Media Management Desk

INACCURATE

Post contains inaccurate information about:
- Government of the day;
- Program
- Events
- Services
- Participants

Or contains media or news questions

- Contact Social Media Management Desk
- Contact Social Media Standards
- Approved Authors respond

LOW RISK

- Offensive Language/inappropriate
- Comments about government officials
- Inflammatory statements
- Criticisms of PM, Ministers, Members of Parliament

- Document Incident
- Take down Page or account
- Talk to person who posted

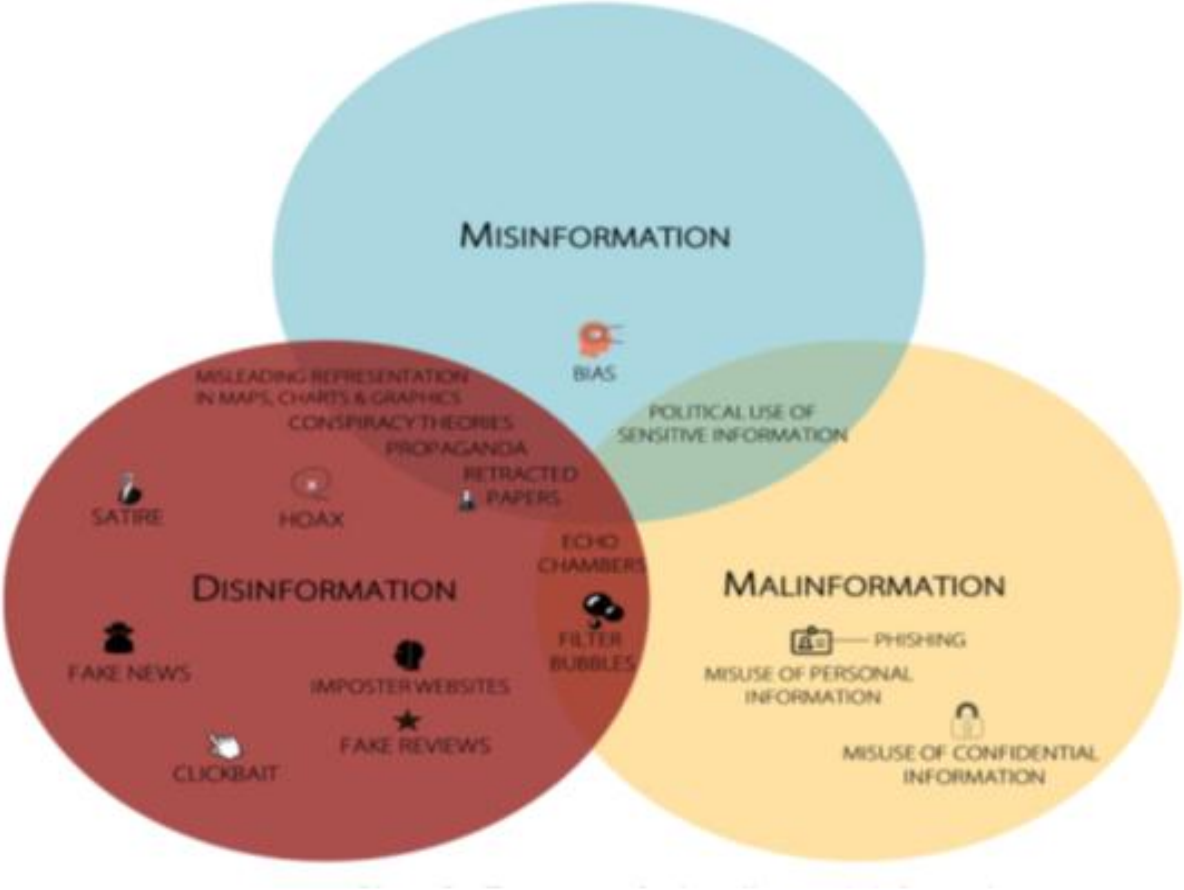
Social Media Management Desk will make decisions on next steps possible including shutting down account, contacting people, consulting cyber crime unit

HIGH RISK

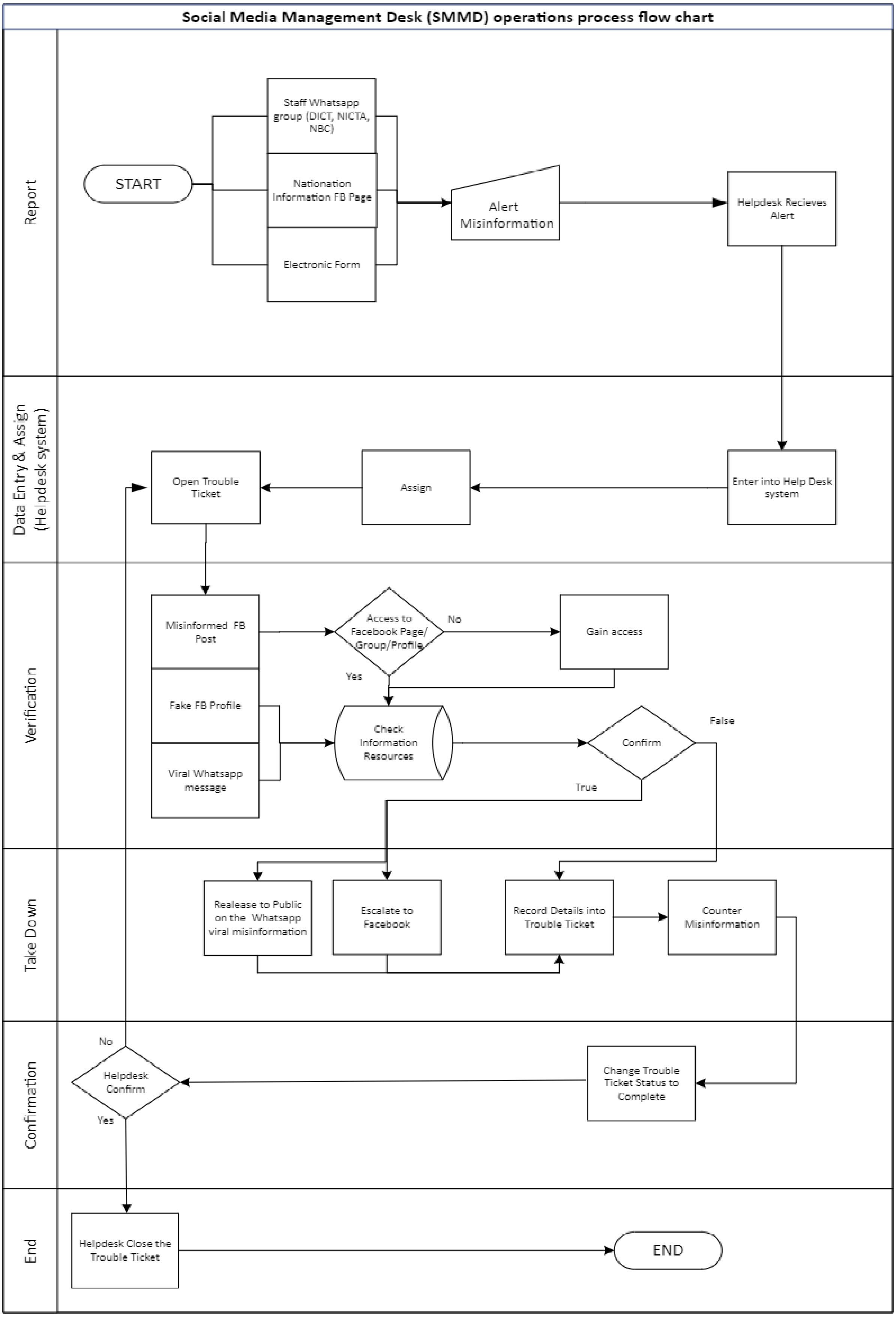
- Inappropriate/violent comments
- Statements with Serious concerns/issues with PM, Ministers, Members and government officials
- Allegations of inappropriate events within the government
- Threatening Post
- Political Group misleading/fake posts

- □ Complete Incident Report
- □ Contact Social Media Management Desk
- □ Document Incident
- □ Take down Page, Account,
- □ Delete Comment or Posts
- □ Flag Comment or Post

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



Annex 2: Social Media Management Desk


Social Media Management Desk (SMMD) operations process flow chart
Report
Data Entry & Assign (Helpdesk system)
Verification
Take Down
Confirmation
End
START
Staff Whatsapp group (DICT, NICTA, NBC)
Nationation Information FB Page
Electronic Form
Alert Misinformation
Helpdesk Recieves Alert
Enter into Help Desk system
Assign
Open Trouble Ticket
Misinformed FB Post
Fake FB Profile
Viral Whatsapp message
Access to Facebook Page/ Group/Profile
No
Yes
Gain access
Check Information Resources
Confirm
False
True
Realease to Public on the Whatsapp viral misinformation
Escalate to Facebook
Record Details into Trouble Ticket
Counter Misinformation
Change Trouble Ticket Status to Complete
Helpdesk Confirm
No
Yes
Helpdesk Close the Trouble Ticket
END

Annex 3. Social Networking Sites Security Tips

Facebook	**Security Tips:** 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 athttps://www.facebook.com/help/379220725465972 f) Check also the community standards on Facebook:https://www.facebook.com/communitystandards/?ref=cr
Twitter	**Security Tips:** 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) b. Accounts with protected Tweets require manual approval of each and every person who may view that account's Tweets. c) 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
Instagram	**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 not 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. Update your accounts as per new security tips and guidelines of Instagram. You can find them at https://help.instagram.com/369001149843369
LinkedIn	**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. 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

Annex 4. 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		
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	