Technical Framework for the Use of Social Media Network in Nigeria

Version 1.0

NIGERIAN COMMUNICATIONS COMMISSION (NCC)
Plot 423 Aguiyi-Ironsi Street,
Maitama District, Abuja

June, 2019

Forward by Executive Vice Chairman

The use of social media is no longer the exception but rather the norm. Individuals, businesses and the Government have found social media platforms as one of the most powerful communication tools for engaging the public, marketing, human resources activities, sales, friendship, brand recognition, innovations, research and development, etc. Social media has become such an inevitable force because of its ease of use and appraisal, the ability to reach netizens almost instantly worldwide without recourse to geographical location. Another key motivating factor is the fact that social media, although relatively new phenomena, neither requires new infrastructure nor involvement of ICT department to be created and used. However, with these benefits and gains, also come negative impacts that have the potential to endanger the individual, business or the Government. Some of these impacts include; liability for libel, privacy violations, impairment to reputation, disruption of infrastructure, espionage, sabotage and other cybercriminal effects. So, in as much as social media presents opportunities for accelerated enterprise growth, and improved reputation or recognition, its inherent risks can be debilitating to national security and the economy. It is in this light that my office has put together this Technical Framework for the Use of Social Media in Nigeria as a non-mandatory guide. This framework attempts to provide the baseline for Social Media governance, policy and strategy, procedures and guidelines to help the individual, business or the Government. However, it does not in any way replace existing frameworks, laws and legislation, rather it serves as complementary document for the overall improvement of national engagement in the Cyberspace. We shall keep all avenues open for closer monitoring and assessment of the adoption of this framework. My office shall establish collation of feedback from adopters of this framework to enhance periodic evaluation of its relevance. It is my singular honour therefore to express my gratitude to the cross section of creators of this document and contributors, that aims towards an enduring safer and prosperous digital environment for our society.

Prof. Umar Garba Danbatta *FNSE,* *FRAES*
Executive Vice Chairman and Chief Executive Office (EVC/CEO)
*T*he Nigerian Communications Commission.

Table of Contents

Forward by Executive Vice Chairman iii

List of Figures vi

List of Tables vi

Executive Summary vii

Section 1

Introduction 1

1.1 Scope 2

1.2 Purpose 2

1.3 Audience 2

1.4 Overview of the Framework 3

1.5 Ownership and Leadership 4

1.5.1 Security and Safety of Users 5

Section 2

Framework Core 6

2.1 Goals 6

2.1.1 Definition of Business Objectives 6

2.2 Strategy 7

2.2.1 People 7

2.2.2 Selecting Content 7

2.2.3 Selection of Platforms 7

2.2.4 Steps for Development of Effective Social Media Strategy 9

2.3 Governance 12

2.3.1 Internal Organisational Context 12

2.3.1.1 The Board and/or Management 12

2.3.1.2 Social Media Policy 12

2.3.1.3 Roles and Responsibilities 13

2.3.1.4 Assurance Governance 13

2.3.1.5 Accessibility Governance 15
2.3.1.6 Resource Governance 16
2.3.1.7 Content Governance 17
2.3.1.8 Response and Responsiveness Governance 18
2.3.1.9 Legal and Compliance Governance 18
2.3.1.10 Data Protection Governance 20
2.3.1.11 Privacy and IP Governance 20
2.3.1.12 Monitoring, Analytics and Reporting 21
2.3.2 National Context 21
2.3.2.1 Legal, Regulation and Compliance 21
2.3.2.2 Duties and Responsibilities 23
2.3.2.3 Monitoring, Analytics and Reporting 24

Section 3

Guidelines for Individual Use of Social Media 25

Section 4

Vulnerability, Threat and Risk Landscapes 28

Section 5

Conclusion 30

Appendix A: Top Social Media Network Platforms

List of Figures

Figure 1.1: Model for Technical Framework for Social Media Network. 3

Figure 2.1: Steps for Development of Effective Social Media Strategy. 9

List of Tables

Table 1.1: Model for Technical Framework for Social Media Network.....4

Table 4.1: Vulnerabilities & Threats, Risks and Countermeasures..... 28

Executive Summary

The digital convergence has brought about a fundamental shift of how information is created, treated and disseminated. In particular, Social Media Network (SMN) has emerged as an inevitable and powerful tool, touching both personal and public lives. This paradigm shift cuts across people of diverse age, albeit, it affects each age category differently. The use of SMN has continued to grow rapidly with sites such as Facebook and WhatsApp recording billions of active users, and Twitter microblog generating over 500 million tweets per day, amongst other platforms. SMN therefore, extends an exceptional opportunity for connecting people around the globe for creation and sharing information in ways never foreseen. Evidently, SMN has altered the communication structure defined and re-defined by both initiator and receiver of information. Conversely, it cannot be overstated that SMN is constantly transforming the way in which people connect and interact with each other and the manner in which information is created, shared and distributed for the individual, business and the Government.

The Nigerian Communications Commission (NCC) as part of corporate responsibility to promote open Cyberspace that is secure and safe has put together this Technical Framework for the Use of Social Media in Nigeria. This framework cuts across technical, legal and institutional issues, and it is hinged on the triad of cybersecurity principles; that is, Confidentiality, Integrity and Availability (CIA). The burden to enshrine transparency, correctness, privacy, Intellectual Property (IP), and contain cyber bullying, racial and hate conversations, fake news, copyrights infringements, data leakage and/or loss, economic and national security, amongst others, are genuine concerns of our digital venture. This framework provides the benchmark to assist institutions, Government agencies and businesses as well as individuals to create and implement strategies, policies, standards, guidelines, procedures, etc. for productive use of social media tools. The idea is to provide a common understanding for various stakeholders to make an informed choice about the objectives, platforms and resources to meet corporate requirements whilst promoting safe and secure social media ecosystem.

Consequently, using a three-layer model centred on goal, strategy and governance, this document provides a comprehensive technical framework. *Section 1* provides the foundational principles that guided the development of the framework core in *Section 2*. *Section 3* provides guideline on the personal use of Social Media, Vulnerability Threat, and Risk Landscapes are presented in *Section 4* in the context of social media. The framework is concluded in *Section 5* while *Appendix B* outlined top Social Media platforms.

Section 1

Introduction

Broadly, social media connotes a web-based enabled application platform that enables users to create or share contents interactively and responsively too. Some of the social media examples include: Blogs such as WordPress and TypePad, image and video sharing platforms such as YouTube and Flickr, microblogs such as Twitter and Tumblr, social sites such as Facebook, MySpace and LinkedIn, etc. The common denominator is characterised by the fact that the conversations or contents are essentially user created and managed.

The impact of social media network is evolving rapidly. It is altering the way people connect, create, store, share and respond to information. More so, it is transforming traditional news media to a more interactive and inter–activity media, where audience can supply, comment, discuss and even further distribute the news. In addition, the power of social media lies in its capability to create highly effective platforms, where people can engage and communicate freely anywhere, any time and in real-time as well as in a global scale. Social media has evolved as machinery for building reputation, hiring workforce, generating revenue and gaining customers' confidence. Worldwide, top brands have combatively employed social media strategies to bolster productivity and financial gains. Equally, governments have embraced social media as part of a core approach to engage citizens for enriched democratic dividends.

While social media has presented quite substantial opportunities and benefits, it has also posed social and security risks that can impact the society and national security negatively. For instance, social media presents the tools for data and privacy breaches, false information, espionage, subversion, sabotage, propaganda, data and intellectual property leaks, hate speeches, incitement, bullying, social and political mobilization as well as distribution of malicious software (malware).

Therefore, as a new phenomenon, the necessity is growing for the public and private sectors, Non-governmental organisations and the Government to identify the risks associated with social media network, and comparatively weigh the benefits when deciding to engage in social media. Consequentially, it implies that participation in social media must be considered in the broader context of business goals and objectives while addressing the associated risks.

These underscore the nee d to establish a technical regulatory framework and rules to guide the participation of individuals and corporate entities in the use of social media network that aim to promote security and safety.

1.1 Scope

This framework serves as the context for Social Media governance, policy and strategy, and guidelines to help engage beneficially on the social media platforms.

1.2 Purpose

The Framework does not attempt to replace any existing Information and Communications Technology (ICT) frameworks, legislation, procedures, etc. but to complement in the inclusive national effort towards open, safer and transparent cyberspace.

This non-mandatory Framework is targeted at Individuals, Businesses, Government Ministries, Departments, and Agencies (MDAs), Non-governmental Organisations, Civil Societies, Professional Bodies operating within the jurisdiction of Nigerian Cyberspace.

1.3 Audience

The Framework is national, implying its adoption by Federating States and Local Government Areas is encouraged.

1.4 Overview of the Framework

The idea is to maximize the benefits of social media tools while bringing to minimal the associated risks. *Figure 1.1* pictorially depicts the model structure for Technical Framework for the Use of Social Media Network in Nigeria.

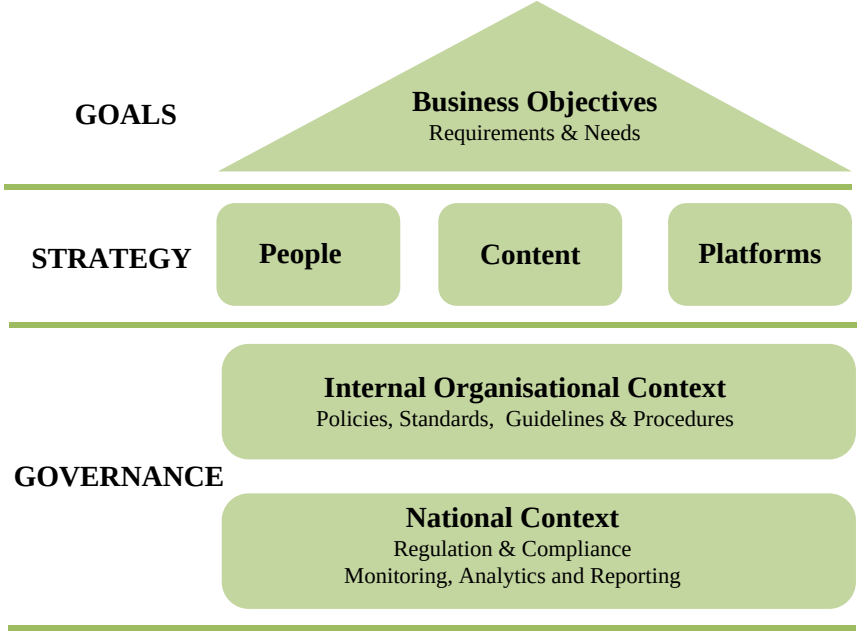

Figure 1.1: *Model for Technical Framework for Social Media Network.*

Goals	The goals define the objectives of engaging in social media platforms. This implies that the purpose, function, and objectives of the use of social media network should be clearly articulated, scoped and defined. Furthermore, the requirement that sets the impacts, which determines the platforms that are selected, the manner they are used, stating the benefits or gains of using social media network to the organisation should be clearly and concisely stated.
Strategy	The strategy defines a set of ways and means for actualising the set goals and objectives that relate to organisational tenet. The essence of strategy is to develop an effective and efficient approach that helps organisations to maximize the gains of social media network while reducing the associated risks. The strategy should be based on a comparative analysis of standards and best practices that help describe the selection of target audience, contents and platforms. In addition, the strategy outlines the techniques for dealing with competitions, positive and negative feedbacks as well as improvements.

Governance	Primarily, governance framework is a vital element that sets out the internal controls organisations can deploy to address the risks of social media usage through the development of policies, standards, guidelines, procedures and best practices that govern the entire social media network ecology. Governance should situate appropriate behaviour in relation to the use of social media tools. Additionally, part of governance framework should address training programs that can effectively and efficiently support correct use of social media by employees. Employees should understand the rules governing acceptable use and behaviour. More so, governance should cut across people, processes, and technology that underpin the entire enterprise ICT ecosystem.
Monitoring and Reporting	Organisations should be able to measure the impact of social media and how it reflects with operational efficiency. This entails that part of organisational strategy should be to create effective mechanism for monitoring and reporting of social media usage. This should include feedbacks that provide insight to what the audience thinks about the organisation's posting and comments and the performance of the engagement. Aside using monitoring techniques to improve organisational engagement, it may be used across the business space of organisation thereby helping organisations make best use of social tools. Organisations can be held liable for the actions of their staff; if staff post false statements, rumours (or fake news) about competitors or colleagues that are damaging on social media, it might lead to potential defamation liabilities. Thus, organisations can install social media software monitoring tools on corporate devices to monitor usage of social media to guarantee compliance to social media policy. Alternatively, organisations can create a dedicated monitoring team that relies on live feeds or streams to screen user's compliance to relevant corporate policy.

Table 1.1: *Model for Technical Framework for Social Media Network*

1.5 Ownership and Leadership

The increasing complexity and sophistication of social media platforms require national ownership and leadership that aim to facilitate appropriate and proportionate regulation, ensure compliance and conformity. The core framework provides the governing principles that define the foundational elements of the framework at national and organisational levels. It describes the role and responsibility of mainstream stakeholders, and delineation of functions and duties to avoid gaps and ambiguity in various oversight functions as well as how to manage the overlap functions. The telecom regulators, news media regulators, financial service regulators, e-commerce regulators as well as security and intelligence agencies, all have roles to guarantee the safe and secure use of social media in Nigeria.

1.5.1 Security and Safety of Users

In order to ensure security and safety of users, users' awareness and education must be included in corporate training calendar. The collaborative efforts to ensure every user has the resources needed to stay safer and more secure online is vitally important. Users must understand what cyber threats are, the potential impact a cyber-attack may have on organisations, and the steps required to reduce risk and prevent cybercrime. In particular,

i. Users must be educated on the cyber threats we all face.

ii. Raise awareness of the sensitivity of resources or systems in the environments we operate.

iii. Ensure procedures are followed correctly by everyone.

iv. Provide information on how to avoid cyberattacks at all levels.

v. Reduce the number of data breaches by tackling vulnerabilities that exist in technology, process and people.

It is equally important to mention that users of social media are aware of the liabilities and obligations associated with social media, and to take necessary steps to minimise the negative impact by imbibing cybersecurity hygiene. More importantly, social media is full of legal concerns, implying that there are potential attributable liabilities; dictating that the risks associated with social media engagement must be thoughtfully considered. The liabilities amongst others may include: libel, slander, defamation, violations of right of privacy, piracy, unfair competition or infringement of copyrights, title or slogan. It then places the obligation on users to ensure as follows:

i. Restraint over false statements or jokes of any nature. The challenge is that social media seems a 'casual medium' prompting users to often make unguided jokes without considering the consequences or impact.

ii. Avoid disclosure of unauthorised content; intentional or unintentional leakage of information of sensitive nature may have legal implications.

iii. Avoid infringement upon other user's copyrights or trademarks.

iv. Avoid spreading rumour or unconfirmed reports (or fake news) that can cause public safety risk.

Section 2

Framework Core

The Framework Core provides a set of activities to achieve specific social media network goals in the form of requirements and needs, clearly, providing the guidance to achieve the anticipated outcomes. The Core is not merely a checklist of actions to perform, it presents essentials of social media network, aiming to help in managing social media security risk. The Core comprises three key elements: Goals, Strategy, and Governance as illustrated in *Figure 1.1*.

2.1 Goals

2.1.1 Definition of Business Objectives

The first step in the use of social media networks is to clearly and concisely define the objectives in a way that organisational goals can be actionable and measurable. It must be understood that social media is not merely to disseminate information but to a greater extent to undertake public engagement meaningfully, such that public participations can form the basis for the formulation of national policy. Government institutions should explore the use of social media for public dialogue for disseminating information, policy making, creating awareness, recruitment, education amongst others.

However, in defining objectives, organisations should be guided by (adopt and adapt) the SMART[1] approach i.e. each objective should be specific, measurable, attainable, relevant, and timely. Essentially, the core objectives of social media can be categorized as follows:

i. Effective dissemination of responsive information;
ii. Platform for soliciting feedback from citizens;
iii. Review, revision or re-pronouncement of public policy;
iv. Specific issue-based interactions;
v. Brand building, promotion or public relations;
vi. Creating awareness on generic issues;
vii. Education on national action plans;
viii. Re-orientation and strong advocacy for national values.

[1] SMART – Specific, Measurable, Attainable, Relevant, Timely -

It should be acknowledged that the determination of the purpose, function and goals of social media by an organisation should have direct impact on the cultural values, selection of platforms, how platforms are used; underscoring the very importance of social media network to the organisation.

2.2 Strategy

2.2.1 People

Businesses and organizations cannot do without people communicating with one another. The objectives, purposes or goals for Social Media activity can be as varied as the organisations engaging in them, but commonly, the set goal is to establish connections, build relationships, amongst people and engage in conversations with diverse audiences whether customers, prospective customers, communities or interest groups, to strengthen and extend information beyond traditional channels.

Therefore, organisation's strategy should be commonly designed to initiate and deepen relationships across one or more precise audiences, such as customers, students, strategic partners, and stakeholders. Its focus should be an extension of existing organisation's services, research and developments, and public relations. The ideal situation is to enable organisation's departments to "go social" where the external visitors expect to find and engage with the organisation's line of bossiness.

2.2.2 Selecting Content

Organisation's strategy should align with the core values, vision and mission, but pointedly, leveraging the SMART to be more engaging, interactive and responsive. Each objective and selected channel should have specific parameters or metrics that define the effectiveness in relation to the goals. It is important to pinpoint that the effectiveness of Social Media Strategy is dependent on exceptionally focused content that delivers information of value to the target audience, and provides novel but unique content that appeals to how the audience perceive things and what they consider important to them. The strategy should convincingly use multiple touch points to achieve the set objectives connecting with audience in fashions that seem natural to them.

2.2.3 Selection of Platforms

It is important to underscore that social media is evolving as well as changing dramatically. It is no longer a way for people to connect and communicate rather is growing as a powerful tool that individuals, businesses and Governments take advantage of, to nurture their audiences, involve customers or citizens for a variety of reasons including increasing revenue.

While social media is developing into farfetched opportunity, it is also growing more sophisticated and complicated. The consequence is the gamut of options to choose from. Does the organisation need an Instagram profile or Snapchat or both, for instance? Should the organisation have Periscope, Facebook and Twitter accounts, and to what degree? How will the organisation know where to direct their time and resources for optimal engagement? Therefore, the requirement for selecting the right social media channels is critical, irrespective of the user being an individual, business or Government. The end goal of every organisation differs, different brands have different goals; an organisational goal may be strictly conversion-based or to increase revenue. In whichever case, the focus should be based on analytics and goals. It is pointless basing the selection on traffics alone, but to as whether the channel is converting and meeting the organisation's needs.

Consequently, an organisation should identify and select platforms that adequately meet the stated objectives, the target audience demography as it may not be effective to engage in all the social media channels. Moreover, different departments within an organisation may engage in different channels. Each social media channel is unique and may require unrelated content, varied kinds of engagement, and assortment of activity. For instance, the Support Department may engage in YouTube to show customers or citizens how to use particular features of organisation's service while the Public Relation Department engage in Facebook and Twitter to tell the public about achievements of the organisation. A clear decision should be made as whether these various Departments or Units will use existing external platforms or create their own communication engagement channels. The factors outlined below provides guidance on the selection of platforms:

i. ***The Duration of Engagement****:* the engagement is meant for a specific time-bound activity or a part of ongoing corporate activity.

ii. ***The Scope of Engagement****:* scaling the engagement as to whether it requires hourly, daily, weekly, bi-weekly, etc. interaction.

iii. ***Target Audience:*** whether the engagement is open to the public or restricted to a particular group of stakeholders or industry. Equally important is where the target audience spend most of the time.

iv. ***Existing Laws or Legislation*****:** considerations should be given to whether existing legislation or laws authorise the use of such media, and if there are requirements under which such laws operate in relation to use of personal data – privacy, data protection, national security, retention and archiving, etc.

An important aspect is that whichever social media channels the organisation choose to participate in, activeness, real-time engagement and consistent quality content are crucial to sustain the organisational visibility.

2.2.4 Steps for Development of Effective Social Media Strategy

The development of an effective social media strategy is very challenging because of the evolving nature of various social media network types, and the varying requirements of businesses and organizations. Taking cognisance of the recommended Technical Framework, the section that follows outlines the steps that should guide the development of effective Social Media Network Strategy.

Figure 2.1: *Steps for Development of Effective Social Media Strategy.*

I *- Identify*

The first step is to identify the objective, goal and purpose of a particular social media campaign in a clear and concise way. Define ownership and leadership structure that is accountable with measurable outcomes.

II *- Audit and Analyse*

The second step is to assess the current status of each of the social media usage and effectiveness if any. The steps that guide this phase of activity is as follows:

a. Documentation of all the social media channels, owners and the URL[2] to profile.

b. Use appropriate search engines, to conduct online search of social imposters, profiles, and analyse in order to determine whether to shutdown the page or not.

c. Evaluate the needs of all social media profiles and create a mission statement for each objective as well as for the channels (*for instance:* Instagram profile – to share organisations values and achievements).

d. Assess the accuracy of brand features of all social media accounts i.e. profile photo, cover photo, icons, bios and descriptions including the URL.

e. Assess access ownership – how is the account accessed and by who.

[2] Uniform Resource Locator

III - *Create/Improve*

The third step is to create a new account and profile or improve an existing account by updating and refining the profile based on the audit and analysis phase. It should be noted that each social media channel has a unique audience, as such should be treated in a different way. Develop this stage bearing in mind that social media profiles should be concise, accurate and that images and text should be optimized for the particular social network channel chosen and for generation of expected traffic. Furthermore, devising cross-promoting social accounts is recommended for extending the reach of the content.

IV *- Content Plan and Editorial*

This strategy develops the content plan, content creation and curation, editing and editorial calendar. In doing this, the plan should answer questions as follows:

a. What types of content the organisation anticipate to post and promote on a particular channel.

b. How frequent the organisation will have to post content?

c. The target audience for each type of content.

d. Ownership and who will be responsible for creating the content.

e. How the organisation will promote the content.

The editorial calendar attempts to schedule the dates and times the organisation intends to publish the content at the selected channels. The idea of the formal structure is to give ample time for procedures and approvals where necessary. The content should be carefully developed and aligned to organisation's ethics and culture.

V - *Developing Content*

This step requires effective research to establish what others in specific sectors or industry is sharing, and the kind of results achievable. The idea is to ascertain the kinds of content and information that will be more effective to engage the selected target audience. Use the concept of Social Media Listening[3] to develop unique culture of a motivating content. The whole idea is to focus on organisation's brand, noting and tracking of trends in organisation's sector or

[3] The process of finding and assessing what is being said about an organisation, topic, brand, or person on social media channels.

industry in order to assess what the competitors/adversaries/opponents are posting about the organisation. Determine the kind of content or information is getting the most ***likes*** on the media, determine if there is the need for countermeasures in the case of directed postings that has the potential to impact the organisation negatively. The driving philosophy is the fact that when an organisation is not paying attention to what target audience is saying, it may unwittingly divulge key content or information that can be valuable to competitors/adversaries or opponents, etc. It is important to present what matters to the audience such as "pain points" in the case of customers, target audience preference for products and services, current wave of talking points specific to the sector or industry.

In general, social media listening mechanism can be the basis for real-time intelligence on competitors/adversaries or opponents, obtain instant valuable feedback, generate actionable data for designing, updating or refining social media campaigns.

VI - *Test, Evaluate and Refine*

This phase deals with continuous testing, evaluation and improvement of social network media campaign formally and structurally, with tools and techniques that can help measure the effectiveness and efficiency of the social media network operations using the defined metrics. Organisations should develop a test plan, evaluation plan and update plan thereby building capabilities into every action the organisation takes on social networks. For example, Organisations can:

a. Track the clicks counts on a particular channel employing tools such as URL shorteners[4] and UTM codes[5].

b. Use tools such as Google Analytics to track page visits.

It is important to underscore that a strategy is not static but must constantly undergo reviews as new channels emerge or digital forces change. Part of this phase should include risk and change management processes that provides guidance for reviews of various segments of the core corporate strategy.

[4] A URL shortener traditionally converts a regular URL into a more compacted format i.e. it takes a long URL and shorten them.
[5] A UTM code is a simple code that you can attach to a custom URL in order to track a source, medium, and campaign name. UTM code enables Google Analytics to tell where searchers came from as well as what campaign directed them to you.

2.3 Governance

The balance between benefits and risks can be addressed by effective corporate governance structure that depicts strong accountability across social media network portfolios. The aim of governance is to ensure that social media objectives are accomplished, resources are well managed, and stakeholders' interest are protected and reflected in key decisions. In this context, governance situates the process whereby an organisation makes informed decisions, control who may be involved in making such decisions and how to ensure reasonable accountability. Furthermore, due to its inherently public nature and worldwide accessibility, effective governance ensures that risks arising from social media engagement are managed consistently, and at the same time enables making the most of the opportunities it brings while constantly staying ahead of change. In this section, guidance is provided on governance structure and processes that underpin rules, procedures, conventions and ethics that governs the use of social media networks. Governance in this context is viewed from national and organisational (stand points) perspectives.

2.3.1 Internal Organisational Context

2.3.1.1 The Board and/or Management

The board or top management must authorize and give approval for social media engagement in a fashion that organisational wide risks are well understood, benefits and gains are understood, and ownership, duties and responsibilities are well defined. More so, the board should take responsibility for the operational mode – whether centralized or distributed across departments, and should be implicitly stated in organisation's social media network strategy and policy documents. The endorsement of social media strategy, policy, standards, guidelines and procedures by the board; ensures that investment in social media engagement is appropriate.

2.3.1.2 Social Media Policy

An organisation MUST develop a social media network governance policy, standards and best practices, guidelines and procedures to ensure that risks and myriad of benefits are balanced comparatively in coherent manner. The policy as a corporate rule provides guidance on the components that form corporate governance toolkit. The toolkit can help address risk to organisation's reputation, reduces confusion about foggy legal issues, and raise awareness across the organisation. In clear terms, the governance toolkit should spell out the boundaries of social media network engagement across every department. It is imperative to mention that no one is immune to the perils of social media, controlling the downsides of social media that minimizes risk by creating a clear governance structure is unavoidable.

2.3.1.3 Roles and Responsibilities

The inimitable nature of social media entails that responsibility for managing and mitigating risk cannot be trivialized. Depending on how the organisation manages other risks, for instance, in managing financial risks, such as keeping trail of regulatory, fraud, and interest rate fluctuations, the Chief Finance Officer (CFO) usually takes responsibility for ensuring that financially focused risks don't expressively affect the organisation. Conversely, since social media risks can spread across departments such as marketing, IT, communications, legal, audit, and human resources, it requires a harmonized and centralized leadership for oversight responsibility.

Therefore, the first step is to create a Unit (or Department) in charge of Social Media whether the organisation's social media network is centralized or spread across departments. The Unit, which should be directly under CEO's office, should be headed by a directorate cadre officer. The Unit should serve as a focal point and coordinating element in charge of all matters pertaining to social media network including, policy directives, strategy, standards, guidelines, procedures, and monitoring and analytics duties. In distributed model, boundaries should be set amongst participating departments and leaderships appropriately delegated. Consequently, the roles and duties of team(s) assigned for creating, managing and responding to social media interactions must be clearly defined in the policy document. The role definition should include amongst others as follows:

i. Escalation mechanism and workflow
ii. Maintenance of access ids and passwords
iii. Data and privacy security
iv. Content integrity
v. Accountability

2.3.1.4 Assurance Governance

It is momentous to validate and monitor all aspects of the framework to guarantee that its elements are, and remain operative and that compliance of relevant controls is established and gaugeable. The essence is to ensure that risks are being managed suitably, that is, social media risks have to be viewed from the People, Process and Technology, relating to strategy and governance.

Technology

The IT department has to establish the relevant mechanism and the supporting capabilities in order to manage technical risks associated with social media engagement. In particular:

i. Technical controls and processes should effectively support social media framework including policies, standards, procedures, etc. These controls should be verifiable to ensure that required technical controls are in place, and functioning correctly as expected.

ii. The IT department should create technical measures to counter malicious codes and attachments using appropriate techniques including network-based and host-based controls to alleviate risks presented by malware.

iii. Controls such as download restraints, browser configurations, content monitoring and filtering, data leakage protection, antimalware products should be put in place.

iv. Suitable technical incident response plans should be created to address any security breach or infection outbreak.

v. A process should be created to mitigate the risk of illegal or unauthorized use of the entity's image or brand on social media or other reproachful postings/comments, which can have negative impact.

Process

Effort should be made to align social media policy and strategy with business processes, in order to ensure that sensitive information is not unwittingly or wittingly exposed. Adequate change controls should be established to ensure that changes or additions to processes that leverage social media are aligned with relevant frameworks including policies and standards before actual implementation.

People

Effective training should be conducted for all users with regular awareness briefings regarding vulnerabilities, threats and risks on the one hand, and policies, standards, etc. on the other. Effort should be made to take off all ambiguity by ensuring that all users understand the boundaries i.e. what is (and is not) suitable, and how to apply applicable protection mechanisms. Moreover, other third parties that may have access to an entity's social media should as well understand their bounds, and the appropriate use of the communication channels, and what information can or cannot be shared.

Risk Assessment

Generally, it is important to establish organisational risks exposure by conducting organisation wide risk assessment that maps social media risks. The aim of the risk assessment is to evaluate the objectives/goals of social media engagement against the business processes for specific platforms. Constantly review fundamental changes to the social media resources in use or when new social media resources are considered for implementation. The objective is to ensure that social media strategy and governance framework can be guaranteed to be effective, constantly reviewing them against the dynamic nature of social media in a manner that is quantifiable.

2.3.1.5 Accessibility Governance

Account Creation

As the term refers, an account creates and binds organisation's online identity. Creation of user account(s) must be consistent across platforms, ensuring that the same name is used for the different social media platforms for ease of search and promoting brand individuality. For distributed models, departments should adopt the same user accounts creation convention. When formulating the account usernames, consideration should be given to the fact that some social media platforms have limitation on the number of characters that can be used. For example, Twitter has maximum of 15 characters long. It is important that credentials are updated regularly, monitored in line with accountability and audit protocols.

Password Creation

Each account requires password, URL, username and/or email address; each of these items should be considered and chosen carefully. Passwords should be simple but strong to ensure that users do not struggle to remember them or compelled to stick them on tables, display units or keyboards. A proper record management should be devised to ensure that sign in ids and passwords are consistently maintained, and consideration should be given whereby multiple users use the same credentials to post on behalf of the departments or the organisation. There is a need to constantly review password requirements in a manner that user experience is not jeopardized. Whenever desirable, depending on the risk factors, consideration should be given to multifactor authentication mechanism to enhance security.

Accounts Integrity

It is critical to define how staff interact on social media, whether mixed account mode is acceptable, whereby personnel can use personal and official accounts to post and respond officially on behalf of the organisation. Accounts integrity should be properly reflected in the organisation's governance policy, standards, guidelines and procedures. It must be clear who says what on behalf of the organisation, and whether in certain circumstance, personnel can respond on personal capacity. Accounts integrity guarantees non-repudiation, which potentially reduces the possibility for reputational damage.

Accountability and Audit

The overall security of social media accounts is preserved in the practice of good security hygiene that ensures confidentiality, integrity and availability. It is important to periodically audit the Domain Name System (DNS), to check misuse, abuse and criminal activity of accounts/users. It is important that security audit be conducted regularly by reviewing specific log files, analysing traffics, inspection of uncommon traffic activities, and then, adequate control measures should be provided to remedy unwarranted events.

2.3.1.6 Resource Governance

It is critically important to underscore the resource intensiveness of social media network campaign, and the resolve to ensure appropriate and proportionate resources are clearly defined and allocated. In the case whereby an organisation intends to outsource human resources, to manage its media platform(s), the terms and condition of such engagement must be well documented and perfected by the legal department of the organisation. Consequently, accountability, responsibility, communications, liability should be marked out very early in the process. Another important key element of resource governance is whether the conversation is moderated or unmoderated, meaning that the policy must have a clear statement on this. In the case of moderated conversation, the moderator(s) should be so selected with appropriate resources allocated. Conversely, alluding to the fact that engagement in social media involves a variety of skill sets, moderators and other resources so identified would need formal orientation and training on constant basis in order to keep pace with developments in the media space.

2.3.1.7 Content Governance

It is important that social media policy document defines clearly content governance structure to ensure consistency and integrity across multiple platforms. It should be noted that social platforms allow everyone to become a content creator, so there is a need for content governance to be well articulated in the policy, procedures and best practice documents, ensuring specific platforms get tailored conversations that aligns with set out objectives. In the case where moderation is important, the structure must be defined in the policy document as to whether others can add content and how, copyright issues, data integrity as to rights to addition and deletion must be clearly stated. Content governance should align with existing rules about enterprise content management, digital asset management, and knowledge management, etc; aimed at gathering, and disseminating knowledge that can help an organization meet set objectives in an efficient manner.

For government Ministries, Departments and Agencies (MDAs), it should be noted in particular that:

i. Conversation on social media is limited to existing government information and propagation of official policy to the public;

ii. Unverified information and frivolous ambiguous facts or rumours should never be propagated through its channels;

iii. Traditional means of communicating to the public should not be abandoned in favour of social media but that social media should be seen as complimenting traditional means of dissemination of information.

Records Management

There is the need to ensure that the creation and dissemination of information follow the common principles of record management; meaning that all appropriate records are captured, trailed and managed properly. It is important to articulate rules that govern record keeping from onset, so that everyone is aware of the status and limitations. Outlined below are factors that should be considered in policy, standards, procedures and guidelines:

i. Record keeping should align with existing regulations, legislation and policy;

ii. Records created should have appropriate tags including creator/sender, dates, posted date, target, etc;

iii. Screenshots of records may be captured and stored appropriately in both hard and soft copies.

2.3.1.8 Response and Responsiveness Governance

Responsiveness is an indication of the frequency at which pages/content can be updated, response can be posted and the manner in which the response can be affected. It should be noted that common fascination of social media is immediacy and spontaneity of response and feedback. This entails that relevant governance documents should articulate the responsiveness and responses within a pre-defined time frame. Contextually, items of importance include but not limited to scope of response (given/not given), response time frame (1 day/1 week), and type of response (official/unofficial). The techniques and tools that can facilitate timely and accurate response should be so integrated in the social media ecosystem. Email and SMS are examples of such tools that can help in this context. In policy creation, it is important to note as follows:

i. Response should align with roles and duties already captured, and in what capacity staff can post response/comments. Respondents should as much as possible maintain an official view as against personal opinion unless otherwise specified, and should be clearly identified, ensuring confidentiality and privacy of data is appropriate.

ii. Not all posts/comments may require immediate response, so timely and accuracy of conversation is critical.

iii. Escalation Mechanism and Hierarchy with typical workflows should be clearly defined for response and queries. Where there is existing corporate response or answer to queries such as FAQ, respondents should point to relevant web resources and repositories.

iv. There should be similarity between responses posted on social media and those of traditional media.

2.3.1.9 Legal and Compliance Governance

It is critically important that the use of social media should take cognizance of existing laws, legislation, policies and regulations, especially the various Cyber Acts, Information Acts, Records Management, data confidentiality and privacy, broadcasting and media, etc. It is imperative that every participant of social media should be made aware of any existing rules and laws to ensure uniformity and consistency in the life cycle of social media management. In particular, participants should be made aware with relevant portions of Cybercrime Act 2015. Some of the key elements that must be taken into consideration are as follows:

i. In the case an organisation runs social media facilities on her network, receives, stores or transmit any form of electronic data on behalf of another party or offers any services in relation to that data, such organisation should be regarded as an intermediary.

ii. From the above, it implies that the organisation is limited to providing access to communications infrastructure, which is made available by the third party, provided the organisation does not:

- Initiate the communication;
- Choose the receiver of the communication, and
- Alter or select the data contained in the communication.

v. The intermediary party should observe proportionate diligence in the conduct of its duty under Cybercrime Act 2015 and take cognizance of other guidelines that may be issued by the government.

vi. The intermediary party MUST not abet or conspire or encourage or induce whether by promises, threats or otherwise in unlawful act under Cybercrime Act 2015.

vii. That on realization or receiving knowledge or notification by relevant Government organisation that data or information or communication link residing in or connected to computing resources is being used to perpetuate unlawful act, must expeditiously disable or delete or remove access to the particular data or information without vitiating the proof in any fashion.

viii. The intermediary party MUST also comply with all other existing regulations, rules and guidelines regarding hosting of social media infrastructure on its network.

ix. The intermediary party MUST exercise reasonable security best practices and procedures under Cybercrime Act 2015.

x. The intermediary party exercise reasonable security safeguards concerning sensitive personal data or information. Sensitive personal data or information considered sensitive consist of information relating to:

- Username/password
- Financial information including bank account details, credit or debit cards other payment appliance details
- Physical, physiological and mental health condition
- Sexual orientation
- Medical records and history
- Biometric information

xi. In general, any organisation either using and/or providing social media facilities, is governed by the liabilities of Cybercrime Act 2015, and any other relevant law, legislation, procedures and guidelines as well as future governance rules as may be applicable.

2.3.1.10 Data Protection Governance

Existing data protection legislation, laws, standards, procedures and guidelines should be observed when communicating through social media and other electronic networks as in non-electronic channels. It should be noted that requirements for data portability compliance may vary from one social media platform to another. In this case, privileged access may be mandated by the government along the same existing laws and legislation, procedures and guidelines for rights infringement and related offences.

It is imperative to note that most of the social media platforms operate outside the jurisdiction of Nigeria, as such not governed by Nigerian laws and legislation, neither managed nor controlled by Nigerian government, thus existing protocols for international collaboration and cooperation may be extended to the use of social media. Furthermore, it may be necessary, if not already exercised that relevant government organisations may engage with the Social Media Service Providers (SMSP) to fashion out:

i. Complaint reporting and response apparatuses
ii. Response time frame for disabling and/or removal of fabricated/offensive contents as short as within 5 minutes but not exceeding 10 minutes
iii. Service level agreement (SLA)
iv. Archival mechanism
v. Shared access of the content
vi. Content storage

2.3.1.11 Privacy and IP Governance

While it may be alluded to the fact that social media attempts to enable grander transparency, it is likewise important to provide mechanisms for the protection of personally identifiable information (PII) and intellectual property (IP) against theft, abuse, misuse and weaponization. Organisations should attempt to create work profiles that are appropriately linked to corporate email rather than individual email addresses to enable social media team administer sites without compromising individual privacy as well as ensuring protection of IP. Organisations should publish their privacy rules in order to ensure that necessary safeguards of users' privacy while maintaining the highest level of transparency. Cyber-attacks through social media, focus on the people element, especially using sophisticated social engineering either by influencing the influencers or hacking their accounts. It has been acknowledged that social media platforms are susceptible to abuse or misuse, especially for the spread of fake news or the alteration of public opinions or perceptions. Similarly, social media can further be used for reconnaissance activities – to gather information that can facilitate attacks on organisations or distribute malware, push rogue antivirus scams and

phishing campaigns against potential victims. Therefore, in order to secure MDAs against social media threats, organisations should as a matter of best practice put in place as follows:

i. An expressive policy, guidelines and procedures on the use of social media;

ii. Continuous awareness and training of staff on the correct use of social media, the vulnerabilities, threats, and risks as well as how unwittingly or wittingly their actions can cause cybersecurity exposure;

iii. Hardening of organisation's network infrastructure technically, to filter or restrict certain content and traffics deemed potentially harmful.

2.3.1.12 Monitoring, Analytics and Reporting

Organisations should make proportionate attempt to listen to conversations on the social media on its behalf. It is critically important to know what users are discussing about organisational brand, how they share and discuss issues relating to the organisation by using social media monitoring tools. There are a variety of off-the-shelf tools including analytics tools in most of social media platforms that can help in monitoring, analysing and tracking of conversations about an organisation. Besides, monitoring is an excellent feedback mechanism to evaluate how organisation's social media strategy is performing. A more appropriate way to handle monitoring is to create a single view social media dashboard to monitor performance across multiple sites.

2.3.2 National Context

Social Media Network has not only strong impact on the society but has national security implications. At the national level, social network requires a governance context that is nationally harmonized and coordinated in order to guarantee the gains and benefits it offers to the larger society. This section deals with the aspect of national context.

2.3.2.1 Legal, Regulation and Compliance

The use of social media undoubtedly comes with inherent risks that have the potential to negatively impact the individual, business and government in ways never anticipated. At national level, the legal implications of the wrong use of social media is an important factor that requires guidelines. In addition, setting the boundaries of what the individual, business and government organs can do and cannot do, as well as how to ensure compliance, are of national interest and a responsibility. In particular, the confidentiality, integrity and availability of social network resources for legitimate use must be assured while protecting

the privacy of personal sensitive information. Some of the important aspects of legal issues are highlighted below:

i. For the purposes of protecting sensitive data including personal data, it is mandatory that any organisation or individual who is processing, dealing or handling sensitive data MUST implement reasonable security best practices and procedures.

ii. The organisation must adopt an industry security standard such as ISO 27001 and comply with its provisions to ensure confidentiality, integrity and availability of resources in line with the provisions of Cybercrime Act 2015. In this case, the organisation does not adopt any security standard, and/or not in compliance with any but has the facilities on which data can be stored, processed or handled, the said organisation should be seen as breaching the law, which may have legal ramifications.

iii. When an organisation provides social media facilities on its networks, receives, stores or transmits any electronic data on behalf of another party or seems to provide service in relation to that data, the organisation should be regarded as an Intermediary Party. Further details can be found in section 2.14.7

iv. Such intermediary party providing social media infrastructure should comply with the provisions of Cybercrime Act 2015, and any other relevant Information and Communications Technology (ICT) rule or act or procedures or guidelines.

v. Where there is a complaint by an individual, business or an element of the Government, the intermediary party should within twenty-four hours on receiving a written complaint from affected legal entity and where applicable, work with the originator of the information to disable, delete or suspend such information, failing to do so may have legal implications.

vi. It is expected that the intermediary party should preserve such data and associated records or links for a minimum of one hundred and twenty days and maximum of one hundred and eighty days for the purposes of investigation.

vii. Whereas the intermediary party does not comply with relevant laws, guidelines, procedures, it may be liable for civil and criminal ramifications.

viii. The civil implications may result to being sued for damages by a way of compensation up to ten (10) million Naira or as may be provided in the Cybercrime Act 2015.

ix. To this extent, stringent requirements of the law, and the consequent legal ramifications for non-compliance of the law, should strongly be considered. It is therefore unequivocally obligatory that an organisation providing social media infrastructure MUST absolutely conform with all the above-mentioned legal strictures as compulsorily specified in this document, particularly section 2.14.7 and Cybercrime Act 2015.

2.3.2.2 Duties and Responsibilities

The proliferation of social media network has evolved strongly spanning across the individual, business and the government, with different set of goals and objectives. While social media presents opportunities, it does have inherent risks that may affect legal entities in a variety of ways with different levels of severity. In mitigating the risks nationally, it is critically important to dispense the duties and responsibilities of mainstay stakeholders in order to avoid clash of interest, ambiguity and negligence. In this context, the various elements of Government by default have statutory duties in the maintenance of law and order, regulatory and compliance oversights, gathering of intelligence to support national economy and security. In the light of the foregoing, it is important these elements of government consider the impact of social media to their traditional roles and as applicable to relevant sections of existing laws, legislation, guidelines, procedures and standards. In particular, sector regulators, law enforcement agents, security and intelligence agencies have national responsibilities for the safe use of social media. The organisations outlined below have natural duties:

i. Ministry of Communication
ii. Ministry of Information and Culture
iii. Nigerian Communications Commissions (NCC)
iv. National Information and Technology Development Agency (NITDA)
v. Nigeria Broadcasting Commission (NBC)
vi. Central Bank of Nigeria (CBN)
vii. Ministry of Commerce
viii. Intelligence and security organisations

2.3.2.3 Monitoring, Analytics and Reporting

In line with section 2.13.1.2, nationally, it is important that relevant agencies create Units or Departments solely dedicated to the monitoring and analytics of social media as a proactive strategy in alignment with existing national security apparatus. Reporting of anomalies and security breaches, and consequent investigations should follow already established protocols and procedures. It is important to note that in the event of a major significant event capable of undermining national security, relevant elements of government should exercise appropriate and proportionate measures to contain such incident.

Section 3

Guidelines for Individual Use of Social Media

Social media has emerged as a vital social tool for an ordinary person, and plays an important role in everyday life. It is now a vehicle and convenient way to access information, provide information and communicate to colleagues, school mates, friends and family. Furthermore, social media has become a platform for building individual brand as most people trust information from people they know; it has become the most effective way to develop trust and authority with target audience. Invariably, the philosophy of social media is the ability to share content and have other connected individuals to re-share the same information to their networks; implying that information going viral is the core characteristic of Social Media.

Consequently, individual users who participate in personal capacity should be aware that inappropriate engagements can have escalated or cascaded effects far beyond their anticipation. Individuals should be conscious that personal communications made via social media are subject to the laws and regulations that govern individual accountability across general and traditional forms of communications. If the individual is an employee, the person should be mindful that he or she represents or is affiliated to an employer in daily living. The individual should exercise absolutely care to jettison the risk of personal and professional matters linking the employer that can bring the organisation into disrepute. The individual personally takes full responsibility for any content personally published - the views and opinions expressed are entirely personal. Thus, the following guidelines provides the individual account users how to promote security, privacy and safety on social media sites:

i. Adherence to existing policies and laws.

The individual should comply with employer's ICT Security Policy and other relevant staff policies as well as the professional codes of conduct relevant to the person's profession (for example Legal Council or Medical Council). The individual should be aware that the obligations to comply with all relevant Nigerian legislation as well as applicable terms and conditions of acceptable use published by respective Social Media site. In particular, the individual be mindful of rules governing access to Social Media sites within employer's network, and should familiarise with details of how to apply, access and use Social Media for work purposes in a suitable policy.

2. No publishing of content of employer.

The individual should not publish content about the organisation where he or she works, its services, facilities, staff, clients or other third entities that could be considered as inappropriate, confidential, offensive, defamatory, discriminatory, harassing, illegal, embarrassing, threatening, intimidating, which could incite hatred or compromise the safety of others or the public. In particular, the individual should 'think', before clicking links, opening attachments even if the sender seems known. Sharing content with care by avoiding to receive or share suggestive contents such as photos or videos. Individuals should endeavour to make Social Network pages private, keeping Personally Identifiable Information (PII) away from the public, and avoid sharing accomplishments that reflect the social responsibility of the organisation as well as personal accomplishments. In other words, individuals should scrutinize the information they share, create or post to social media to minimize the risks of unnecessary data disclosure. In the event individual accounts are not private, cautions should be taken to observe security and safety guidelines already outlined, including ensuring strong passwords are used for the accounts.

3. Whistle blowing

The personal Social Media account is not the suitable place to raise or discuss other people's or work matters or issues. Whereas there are genuine concerns, it should be addressed through appropriate authority at work place or law enforcement agencies.

Other personal advice on the use of Social Media sites are summarised in the following section.

i. The individual should choose network contacts or friends wisely in consultation with ethical guidelines of his or her professional body or work place. Before 'liking' or 'following' others (or deciding whether to permit others to 'like' or 'follow' you), the person should consider whether he or she can to be associated with that person/brand/organisation and their views and values. Consideration for any potential consequences or repercussions that could arise from such association should be thought through to avoid any conflict of interest.

ii. The person should think carefully before publishing any content. This applies to individual content/messages and when circulating other people's contents. It is important to note that status updates can be seen by others, and published content can be difficult to retract, and it circulates very rapidly, perpetually available for others to see and use elsewhere indiscriminately.

iv. The individual should monitor publish/share content area regularly, to check if the public can have access to it, to avoid malicious posts to appear on personal account. Any content that others publish that can be considered inappropriate should be deleted immediately.

v. It is important, the individual exercise caution to keep personal account secure and check personal privacy settings. The person should ensure the awareness of the security settings on personal Social Media account, and regularly review these settings to maintain personal security, privacy and safety. Adoption of strong passwords that have properties such as:

- Long – minimum of 8 characters;
- Mix capital and lowercase letters, numbers, and symbols
- Easy to remember, hard for others to guess e.g. John likes to play football – J!loLikes2PlayF0otball; Strong passwords are safer – Str0ngpa$$w0rdsRsafer!
- Avoid share of password or PIN with anyone including family or friends;

Section 4

Vulnerability, Threat and Risk Landscapes

The social network media as we know it today connects the society with like-minded people – the networks of 'friends' or 'followers', and generally consist of people who share the same values and beliefs. Consequently, these values whether social, political or economic, invariably help to define who we are, and what we believe in. This 'social trust' reinforces the shared sentiments through network of friends or followers, which lies the underlying dynamism that makes the social network media vulnerable with attendant threats and risks. This section provides general overview of vulnerability, threat and risk landscapes, and some countermeasures that can help mitigate against the risks.

Table 4.1: Vulnerabilities & Threats, Risks and Countermeasures

Vulnerabilities and Threats	***Mapped Risks***	***Countermeasures***
Exposure to the public can lead to fraudulent use of corporate identity or brand	Provides source of information that can be hijacked or exploited by adversaries, targeted phishing attacks on staff, partners or customers or reputational damage.	Scrutinize information exposure, use experts to conduct risk assessment that gives holistic view of how an adversary can turn corporate information to its advantage. Create awareness and education across tiers of users appropriately.
Viruses and Malware distribution through the network	Disruption of services (or system downtime), data leak or theft, hijacking of network as zombies (botnets), cost of response and recovery.	Ensure cybersecurity defence in-depth strategy in the network, with constant updates on security patches and upgrades including antivirus and antimalware, content filtering and effective network monitoring of activities.
Undefined conversation and content rights	Unable to track, control contents leading to loss of legal rights.	Certify that user agreements of social media sites are reviewed by the legal and communications teams. Policy document should specify what information that can be posted. There should be mechanism to capture and log all conversations.

Vulnerabilities and Threats	***Mapped Risks***	***Countermeasures***
Use of individual user accounts to communicate official matters	Privacy breach, reputational damage, erosion of competitive advantage	Make a clear policy directive about use of personal social accounts. Ensure HR and Training create the necessary awareness that reinforces policy directive.
Staff postings of unauthorized images or information that link them to the legal entity.	Identity or brand diminishing, reputational damage	Policy directive should be clear how staff use organisation's images or resources/assets including IP in their personal social presence.
Unwarranted use of social media during office hours	Consumption of network resources, productivity loss, potential for increased exposure to malicious codes and viruses.	Policy directive should be clear on the engagement of social media. Technical department can use content filter or other security measures to limit access to social media sites, and only permit those who may have legitimate access to the sites.
Access to social media via organisation-supplied mobile devices (or smartphones)	Loss of mobile device, infection of mobile device, data theft/leakage, hijack of device control	Clear policy directive should be developed on the use of corporate devices. If within organisation's network, ensure that devices are routed through security controls, ensure constant update of devices including antiviruses and antimalware
The use of Social Media to spread fake news, misinformation, propaganda, rumours, hate speech, bullying, etc. has reached alarming state. Certainly, the nuisance of these threats come in many flavours, implying that sensational news and social media campaigns are usually filled with mistruths.	Recent events have shown that social network media can be used to spread or facilitate fake news, misinformation, propaganda, rumours, hate speech, etc. All these threats to the society can sway social, economic or political opinions, polarise the society, propagate divisive and cruel hoax, and alter beliefs, leading to racism, tribalism, harassment, intimidation, and damage to reputations. It can affect international relations, irreparable harm or loss including death of an individual or persons.	Most users seem not to understand the consequences of their actions as many has argued that the whole idea is a matter of perception. The real issue is how to differentiate fake and real content because often users believe that the friends and the platform delivering the content are trustworthy. Currently, there is not acceptable standard or solution to curtail 'misleading content', however, some steps as follows can help mitigate the threats: i. Development of appropriate policy and law; ii. Early release of verifiable content; iii. Monitoring of social network media content; iv. Prompt issuance of counter content by constituted authority using the same media.

Conclusion

The rapid increase of the use of Information and Communication Technology, and the Internet have continued to offer unprecedented opportunity for connecting people together that can create, store, and share information that knowns no geo-borders. Particularly, it has provided communication structures that can be defined and redefined by both initiator and receiver of communications. This is what is referred to today as Social Media Network. Social media network has emerged the most powerful communication tools of our time, characterized by connectedness, audience, collaboration, community, immediacy and interaction in most intuitive fashion. While social media tools have presented unparalleled opportunities for individuals, organisations and governments across the globe as part of corporate strategy for productivity and financial benefits, it also has huge challenges and security risks that have debilitating effects. Therefore, it is imperative for individuals, organisations and governments to continue to enjoy the benefits of the platforms that a technical framework that guides its use has become critically essential. This will greatly increase the benefits and gains while bringing the associated risks to tolerable minimal.

Appendix A: Top Social Media Network Platforms

***Twitter*:** Twitter is a social media network that allows people to share status updates in a short (limited to 140 characters or less), succinct format. A user must create a digital user's account in order to access the site. The platform allows users to build up a contact list and followers; this makes them to receive updates each time the account holder posts a new status. Recently, businesses and governments frequently use Twitter to keep the public particularly their audiences educated about new opportunities, developments, issues and changes.

***Facebook*:** Facebook is ranked the most popular social media network based on its user base of more than 500 million entities. It provides most functionality that appeal to every social media network users, which include status updates, wall posts and private messages. More so, it offers users platform to send instant chat messages. The site is the one site where users are likely to find friends, colleagues, and relatives worldwide. The site offers users the place to build a complete profile with personal information such as photographs, links, videos and favourite items and interests. The site also supports users groups, which allow users to come together based on a particular subject matter, cause, issue or interest.

***LinkedIn*:** LinkedIn is a professional focused social media network platform, mainly used for professional networking, including organisations posting vacancies and job hunters posting their CVs. It has emerged as a platform for meeting customers, vendors, recruiting new employees, and keeping up with the latest in business or industry news.

***MeetMe*:** This site formerly known as MyYearbook, is a site principally focused towards youths. It has a variety of features and activities that makes it attractive to teenagers, specifically to make friends and meet other people. In addition, it has a virtual economy called "LunchMoney" which users can use to buy virtual gifts, stickers, charitable donations, etc. The site is also known for games, television shows, and image battles.

***Xing*:** Similar to LinkedIn, is a professional networking and recruitment platform with global presence and emphasis. In addition, the platform has a variety of features and groups that make it situated for developing relationships with vendors/suppliers, colleagues and industry leaders.

Renren: Literally meaning "everyone's website," it is China's largest social site. Its functionality and features is similar to Facebook, which allows users to create and share information quickly, update their status, connect with others, and add posts or ideas. It is largely popular amongst the Chinese youths.

***Google+*:** This is Google's social site that combines the best of features and functionality of Facebook and Twitter into a single view. With the powerful world's most popular search engine, it helps users to quickly build circle of friends, colleagues and others communities.

***Snapchat*:** It is an image messaging social site that enables users to chat with connected people by using pictures. It basically offers the ability to take a picture, add art and text, and then post it to recipients within a set time, after which the image will delete itself and be removed from the site's servers.

***Tumblr*:** This site is significantly different form most of other social platforms; basically it hosts microblogs for end users thereby allowing individuals and businesses to fill their blogs with multimedia (like photos and short video clips) as viral content.

***Pinterest*:** This site, which is popular amongst women offers the platform to share images, creative thoughts, particularly photo projects that other connected users can pin, save, or even duplicate. As a giant virtual impression and inspiration board, it has made an incredible impact on social media network.

***Twoo*:** This social network site originated from Belgian has normal social features such as posts, updates, and photo sharing, online games and chat features targeting younger users who are likely to want to be entertained whilst connecting with equals.

***MyMFB*:** Similar to Facebook but specifically created for Muslim's alternative to Facebook, aiming to interconnect over 1.5 billion followers into a single social platform. It is rapidly growing and offers a variety of the same post, update, and sharing features as the original Facebook, and is fast becoming popular in certain parts of the world.

***YouTube*:** This site provides billions of people the platform to discover, watch and share originally-created videos. It is a platform where people connect, inform and inspire others worldwide. Equally as a distribution channel for those who create original video content and promoters including individuals, small and large firms. The platform features first-person product reviews to advertising clips and "how-two" lessons on practically every topic or discipline.

***Instagram*:** This site provides a quick and convenient way for connected people to snap and share images from the camera feature of the smart phone and link with all other social profiles. It instantly allows users to share via Twitter, Facebook, and the Instagram website, also using a variety of photo filters as well as the capability to invite connected people to comment on photos or ideas.

***Vine*:** This site, which offers users the channel to share and view short-lived video clips is entertainment-focused, with a substantial favourite towards "viral" and "meme" clips that can be shared easily.

***WhatsApp*:** The WhatsApp concept is simply a messaging platform that combines text-style messages, conversation via live telephone or video calling. The platform has the capability to create groups and communities, making the platform the world's most popular messaging platform.

***vk.com*:** This site is typically the Russian form of Facebook, featuring the same types of profiles, messaging, and games. Similar to Facebook, **vk.com** offers users the place to post both personal and professional data about themselves, and to follow or show support for organizations and businesses.

***Meetup*:** Meetup as the name suggests is known for organising local groups around particular interests. The interests vary including music to hobbies, and get-togethers to attract newcomers.

***Medium*:** This site is known for an ongoing, up-to-date "how to" instructions written by the expert professionals. It is very rich in helpful advice, tips, and articles that can help advance knowledge in a particular area.