FEDERAL GOVERNMENT OF NIGERIA

NATIONAL INFORMATION TECHNOLOGY DEVELOPMENT AGENCY

Standards and Guidelines for Government Websites

1.0 INTRODUCTION

1.1 Authority

In exercise of the powers conferred on NITDA by section 6 of the National Information Technology Development Agency Act of 2007, NITDA hereby issues the following Standards and Guidelines for Government Website.

1.1 Explanatory Notes

Effective communication with the citizenry is one of the fiduciary responsibilities of all levels of governments in Nigeria. For several decades following Nigeria's independence from British colonial rule in 1960. The Federal Government Press was the primary publisher of government information, including gazettes issued by the Nigerian Public Service. The growth of the internet has enabled many Nigerian Government Institutions to publish individual websites about their organization's mandates, structure, programs, projects and services. Some Government Institutions have gone as far as providing online services to meet the growing needs of Nigerian citizens. The rapid growth of mobile and internet penetrations in Nigeria has enhanced the capacity of citizens to access online services offered by the Government Institutions. In addition to improved availability of government information, government websites have equally increased the capacity of Nigerians to participate in public affairs, thus strengthening the relationship and credibility of governance processes.

The popularity of websites among Government Institutions has some challenges too. The first is the high level of inconsistency in the look and feel of websites owned by Government Institutions. Government websites have come in varying levels of quality, and scope. Others areas of inconsistencies are structure of navigation, writing style and terminations used.

1.2 Scope

The objective of this document is to provide standards and guidelines for the development and management of Government Websites thereby improving the quality, reliability, accuracy and accessibility of online information pertaining to Government Institutions at all levels of government and to ensure consistent experience for all users.

The specific objectives include the following:

1. To ensure that Government Institutions meet the broader communication objectives of the Government of Nigeria
2. To ensure that Government Institutions' websites are updated, maintained with accurate content for public consumption on a regular and timely basis
3. To ensure that Government websites are usable and easily accessible by the citizens
4. To ensure consistency in design and domain nomenclature for all Government Institutions' websites
5. To guide IT personnel in designing, developing, managing and securing the websites within their respective Government Institutions
6. To enable users of government websites access credible information in a manner consistent with global best practice.

1.3 Principles

All Government Institutions should consider the needs of a broad spectrum of visitors, including general public, specialised audiences, people with disabilities, those without access to advanced technologies, and those with limited English proficiency and ICT skills.

1.4 Definition of Terms

Acrobat Reader: A standalone computer program, mobile app or web browser plug-in from Adobe Inc. that provides the ability to view a Portable Document Format (PDF) file in its original form and appearance.

Access Provider: An organization that arranges access to the Internet through a Dialup account.

Address: The unique identifier needed to either access a website (see URL) or to send email.

Applet: Small program embedded in an HTML page usually written in Java.

Bandwidth: The maximum data transfer rate of a network or internet connection. This is typically a measure of how much data can be transferred over a stipulated timeframe usually in seconds.

Bookmark: A web page that is added to a browser list for easy access.

Bounce: Return of an email because it could not be delivered to the specified address.

Browser: Tool (software program) that allows users to 'surf the net'.

Cache: An auxiliary memory that enables high speed access for computer programs

CGI: Common Gateway Interface: Interface that allows scripts (programs) to run a web server. CGI scripts are used to put the content of a form into an email message, to perform a database query, to generate HTML pages 'on-the-fly', etc. The most popular languages for CGI scripts are Perl and C.

Compression: Technology that reduces the size of a file to save bandwidth and memory usage.

Cookie: A small file deposited on a user's local hard disk to track activities of a particular website.

Deep Linking: Creating a link that points directly to a web page or other content within another website, bypassing the opening page or other identifying pages.

Dial-Up: A connection or line reached by modem.

Domain Name: A unique name that identifies an internet website. A domain name points always to one specific server, though this server may host many domain names.

Download: Transfer of data from a server to a user's computer hard disk.

e-Commerce: The process of conducting a financial transaction through electronic means, e.g. using debit or credit cards, purchasing goods over the internet.

EFTPOS Electronic Fund Transfer at Point of Sale: An electronic fund transfer which involves the use of debit or credit cards

Email: Messages, usually text, rich contents and attached files, sent from one person to another via computer. Email may also be sent automatically to a large number of addresses (using a mailing list).

FAQs: Frequently Asked Questions

Firewall: Internet security to protect a LAN (Local Area Network) against hackers. A combination of hardware and software act as a firewall to separate the LAN into two parts. "Normal" data is available outside the firewall, while more private and confidential material is inside.

Forms: In this context, electronic forms that can be filled in for different purpose (e.g. providing feedback, registering for a service).

Freeware: Freeware are generally software which are distributed for free, and may or may not be copyrighted (conditions may include an obligation to redistribute the software for free or not)

Shareware: Shareware is distributed for free, but often in a limited version, requiring payment before the software is used. Some shareware are unlimited, relying on users to be honest about whether they pay for it, but the legal obligation is clearly presented in the software.

FTP: File Transfer Protocol: a common method of moving files between two internet websites. FTP is a special way to log in to another internet website for the purpose of retrieving and/or sending files.

Gateway: Hardware or software that translates between two dissimilar protocols.

GIF: A lossless format for image files that can contain both animated and static images.

Hits: A count of all successful hits on a website. It is not recommended as a means of counting website usage. 'Sessions' provide a more accurate analysis of the number of users who have visited a websites. Sessions are typically unique and categorized into returning and new ones.

Home Page: The primary or main page of a website

Host: The server on which a website is stored. Hosting companies store websites of their customers on powerful web servers (with fast, permanent connections to the Internet).

HTML Hyper Text Mark-up Language: the coding language to create hypertext documents on the web. HTML represents formatted text which web browsers can understand and represent in more human readable forms

HTTP Hyper Text Transport Protocol: the protocol for moving hypertext files across the Internet.

Hypertext: Generally, text that contains 'links' to other documents.

Internet: A network of computer networks that communicates using TCP/IP protocols.

Intranet: A 'closed Internet' for internal use only also utilizing TCP/IP protocols

IP Internet Protocol: the rules that provide basic Internet functions. IP allows computers to find and interact with each other.

IP address (IPv4): A 32bit Internet address consisting of four numbers, separated by dots and sometimes called a "dotted quad". Every server connected to the Internet has an IP address.

IPv6 address: It is an enhanced form of IPv4 address which allows for a larger number of nodes

IRC Internet Relay Chat: A chat network where the words are written rather than spoken. All words typed by any user are seen by everyone who is in that "chat room" at that moment.

ISDN Integrated Services Digital Network: Facilitates high-speed transfer transmission (up to 128 Kbps) of voice and data.

ISP Internet Service Provider: A company that offers access individual and organization users access to the Internet

JAVA: A platform independent programming language invented by Sun Microsystems (Now owned by Oracle Corpoeration) that software engineers use to create desktop applications, mobile applications and applets that leave inside browsers. Although many software developers prefer Java because of its possibilities, there is the need to take into consideration that many web browsers disable Java by default due to security risks.

JavaScript: An object oriented programming language usually used to develop very rich interactivity within websites. More recently, Javascript can be used to write server-end application using the node.js framework and also used to develop mobile applications by employing frameworks like PhoneGap, Cordava e.t.c.

JPEG Joint Photographic Experts Group: Image compression standard, optimized for full colour (millions of colours) digital images. The amount of compression can be chosen, but the higher the compression rate, the less quality the image has. Almost every full colour photograph on the web is a JPEG file, while GIFs are used to display clipart images.

Log: A file that keeps records of a website's or a server's activity. The file that contains information on how many visitors a web page is getting.

LAN Local Area Network: Two or more computers connected together via a network, usually by cables.

Mail Server: A server application that handles incoming and outgoing email usually hosted in a physical or virtual server.

Mirror Website: More or less an exact copy of another website. Mirror websites are created when the traffic on the original website is too heavy. They are usually on servers that are located in different geographic areas.

Modem Modulator & demodulator: A device that connects a computer to a phone line, fibre line or coaxial line enabling access mostly by converting analogue to digital signals

MPEG Moving Pictures Expert Group: Compression standard for video in a format similar to JPEG.

Newsgroup Discussion group amongst people who share a mutual interest. In any particular newsgroup one can find several

conversations on different topics. There are thousands and thousands of newsgroups, covering almost every possible subject.

Online: In this context, actions performed when connected to the Internet.

Online services: Services accessed through the use of electronic technology, with an emphasis on Internet and telecommunications technology.

Page views (Impressions): Total hits on a particular web page of a website

PDF Portable Document Format: A file format that captures all the elements of a printed document as an electronic image that can be viewed, navigated, printed, or forwarded to someone else.

Protocol: An agreement relating to systems which allow computers to communicate together. TCP/IP protocols define how computers on the Internet exchange information.

Rich Text Format (RTF): A file format developed by Microsoft in 1987 for use in their products and for cross-platform document interchange

Server: In this context, a host computer providing the website information.

Streaming video: A sequence of "moving images" that are sent in compressed form over the Internet and displayed by the viewer as they arrive. 'Streaming media' means streaming video and/or sound. With streaming video or streaming media, a web user does not have to wait to download a large file before seeing the video or hearing the sound. Instead, the media is sent in a continuous stream and is played as it arrives. The user needs a player, a special programme that uncompresses and sends video data to the display and audio data to the speakers. A player can be either an integral part of a browser or an independent application.

TCP/IP Transmission Control Protocol/Internet Protocol: A suite of communications protocols that defines the basic workings of the Internet.

Users/Visitors Throughout this document, the broad term 'visitors/users' encompasses all those who visit and use the MDAs' Websites and online services

URL Uniform Resource Locator: Address of any resource on the World Wide Web.

Visitor Sessions Total: A count of the visitor sessions to the website.

Visitor Sessions Average: Average number of visitor sessions per day. The number of visitor sessions divided by the total number of days in the log.

Website: A web page is a document with a single URL. A website is one or more web pages with a related set of URLs that are identified with a single domain name.

W3C: World Wide Web Consortium

2.0 NIGERIAN IDENTIFIERS

2.1 Nigeria Government Identity

Government Institutions should ensure that information published on their websites are authentic, reliable and credible. All Websites under Nigerian Government Domain at any level (Federal, State and Local Government level) must prominently display a strong Nigerian Identity and ownership of Nigerian Government. In order to achieve these objectives, the guidelines stipulated below shall be adhered to:

1. The National emblem (Nigerian Coat of Arms etc.) should be displayed on the homepage of the websites of all Federal Government Institutions. The use of the National emblem such as the Nigerian Coat of Arms, should be in accordance with the provisions of the Nigerian National Flag and Armorial Ensigns Act of 1962.
2. Government Institutions shall display their official logos on the homepage of their respective website to re-enforce their identities.
3. The homepage and all important entry pages of the website shall display the ownership information, either in the header or footer.
4. The ownership of the Agency should also be indicated at the bottom of the homepage and all important entry pages of the website. For instance, at the bottom of the homepage, the footer may state the lineage information, in the following manner:
    a. This Website belongs to *National Information Technology Development Agency (NITDA)*
    b. This is the official Website of *National Information Technology Development Agency (NITDA)*
    c. This is the official Website of the *Ministry of Communications*
5. Government Institutions shall ensure that all subsequent pages of the website display ownership information in a much simpler form as possible.
6. All website home pages MUST be complete and clearly display the name of the respective Government Institution or Service.

2.2 Government Domains

2.2.1 General Information

The Domain name and all uniform resource locators (URL) of any Government website is a strong indicator of its authenticity and status as being official.

All established, commonly acceptable Domain Name Service (DNS) naming convention by NIRA www.nira.org.ng MUST be complied with. Government Institutions with complexity in their names shall try as much as possible to establish their online identities while minimizing complexities of choosing a name.

2.2.2 Domain Nomenclature

Domains under *.gov.ng* shall be registered under the rules and guidelines set out by NIRA in its Domain Name Policy documents www.nira.org.ng. The following examples can be a guide:

NO.	INSTITUTION	DOMAIN FORMAT
1.	Federal Ministry	MinistryName.*gov.ng*
2.	State Government	StateName.*gov.ng*
3.	Agencies	AgencyName.*gov.ng*
4.	Departments	Department.*gov.ng*
5.	State Government Agencies	AgencyName.StateName.*gov.ng*
6.	Nigerian Foreign Missions	CityName.mofa.*gov.ng*
7.	Institutions	InstitutionName.*edu.ng*
8.	Military Establishment	OrganizationName.*mil.ng*
9.	Government Services (e.g. gifmis.gov.ng, fgnzbb.gov.ng, npower.gov.ng)	NameOfService.*gov.ng*

In compliance with the Government Domain Name Policy, all Government Websites must use .gov.ng exclusively. The above naming Policy applies to all Government Websites irrespective of where they are hosted. Also based on the extant rules as stipulated in the Regulatory Guidelines for Nigeria Content Development of 2013, all Government Services and Websites must be hosted in

Nigeria.

2.2.3 Guidelines for choosing a Domain name

NIRA has set out Domain Name naming convention as contained in www.nira.org.ng with much clarity. Government Institutions with complex names that cannot easily conform to NIRA's policy documents should choose a suitable domain name that is not at gross variance to the basic naming convention policy of NIRA. Such selected names shall as much as possible to reflect the names or brand to which the name is chosen for.

A set of guidelines for selecting a suitable domain name to align with the overall policy on registrations of domains under the *Top Level Domain (TLD) for Government* (*.gov.ng)* is given below:

i. Choose a single short name that establishes the identity of the Government Institution or Service, provided that the name is not a common/generic name shared by two or more Government Institutions or Services (e.g. Communication, Education, Defence).
ii. Choose abbreviations that are easy to remember (nitda.gov.ng, buk.edu.ng, navy.mil.ng). This is more appropriate for Institutions or Services that are not temporary in nature.
iii. Prefix or suffix D or M (to denote Department or Ministry) and insert O (to denote of) within an abbreviation to make it more memorable (e.g. moe.gov.ng)
iv. Use shortened forms where acceptable (e.g. meteor - meteorology, exams - examinations)
v. When there are unrelated/multiple subjects assigned to a department, choose the most important or well-known subject (which is less likely to change) for the domain name (department of intergovernmental affairs – intergovernmental.gov.ng)
vi. In case of States and Local Government Institutions where the area name is longer, shorten it in a meaningful and memorisable manner.
vii. Dash or underscore is not recommended.
viii. Characters like $, @, % etc. are not allowed and shall not be used.

2.2.4 Procedure for Registering a Domain Name

All Government Institutions that wish to register domain names shall submit their applications to National Information Technology Development Agency (NITDA) for. ***gov.ng*** domains and to Galaxy Backbone Limited (GBB) for ***.mil.ng*** and

.edu.ng domains. The process of verifying and setting up a domain name should not take more than 7 calendar days from the date of request. Visit www.nira.org.ng for details.

3.0 Information Provision

3.1 Information Provision

The Internet is becoming a preferred means of accessing Government information and services. Therefore, Government Institutions through their websites must make sure that information provided is current, and that it is updated at least weekly.

3.2 Requirements

Information presented on a Government website must be consistent with Government policy to avoid the possibility of misinformation to both Government and the public. If information is incorrect or inappropriate, the application of common information provision standards across Government websites will ensure consistency.

3.3 Level of Information Provision

Government Institutions should publish copies of documents and other information on their websites. Where this is not practical (e.g. high costs, limited bandwidth, low demand, publication complexity), information on how to obtain a copy in its original form should be posted on the website.

3.3.1 Home Pages

Home pages should include the following basic components:

i. Name of Institution,
ii. Logo as appropriate (*in the absence of a logo the coat of arm should be used as the default logo*),
iii. A link to the institutions Principal Officers' page which displays the photo and profile about the Principal Officers,
iv. A link to a contact page that includes information which shall include a functional phone number and a monitored email address on how the Government Institutions can be reached and a form which has the following fields:
    a. Name
    b. Address
    c. Message
    d. Monitored email address of the institution or business unit responsible for public relations.
v. A link to a feedback/comment page
vi. A search facility,
vii. A Site Map should also be included.

3.3.2 Individual Pages

Each page of the website must include a search facility, consistent navigation, and a link to the contact page.

3.3.3 Directories of Services and Organizational Structure

Government Institutions are required to provide full contact details, including physical service locations, telephone numbers, and mailing addresses. Email addresses should also be provided, in particular, for the department or unit responsible for maintaining public relations.

3.3.4 Citizen's help sections

This section shall include information about what citizens must expect from Government and what Government expects from them. It will include the following:

i. Complaints handling processes,
ii. Application, enrolment or compliance forms,
iii. Explanatory notes and policies,
iv. Information about benefits and entitlements.

3.3.5 Forms

Forms widely used by the public should be made available on websites, either in downloadable or online entry formats.

4.0 Content Guidelines

4.1 Content guidelines

For effectiveness in online communication, the following must be adapted in presenting content:

a. Highlighted keywords,
b. Titles and subheadings,
c. Ordered and unordered bullet lists,
d. One idea per paragraph.

4.2 Requirements

To ensure content is suitable for the web:

a. Write succinctly,
b. Make text easy and quick to read,
c. Use plain English
d. Use English and the Local Language of the targeted audience where applicable (e.g. Nigerian Foreign Missions' Websites)

Institutions must always bear the target audience in mind and consider their level of computer accessibility to guide the composition and the presentation of content.

4.3 The Information

Documents published must be suitable, clearly written, unambiguous and must not be malicious. Graphics should be used sparingly as it increases download time.

4.4 Content

4.4.1 Creating Content

In creating and presenting content, establish a clear information structure, limit each page to one concept each, and apply the same principles of plain English and inclusive language to websites that apply to printed documents.

4.4.2 Writing Style

Website writing must use plain English. It must avoid acronyms, jargons, and complex words. Content must not be offensive. Use correct punctuation and be sure of spelling correctness. Use bullets and listings as may be required.

4.4.3 Text Formatting

The following should be adapted for text formatting:

i. maximize readability by making text left-justified, except where other forms present a suitable layout
ii. use the bold font style for highlighting or emphasis
iii. avoid underlining text, it can be mistaken for a hyperlink
iv. avoid using coloured text, this may be difficult to read or present difficulty for the colour blind. It also may confuse the reader to think it is a link
v. italicize references to published documents such as Reports, Frameworks, Acts, Policies, etc.
vi. headings should be in sentence case format, with the initial letter of the first word capitalized, with all remaining letters except for proper nouns in lower case
vii. date, time, currency, telephone and location information should take into account the geographic location of users.

4.5 Quality

a. Processes need to be put in place to ensure that the content created for the needs of the website is of high quality, accurate, current, meets the needs of the public and the requirements of Government.
b. Each information resource and service should have an owner (a person or unit) who has continuing responsibility for the quality, accuracy and timely update of the information.
c. Overall, Government websites should recognize the target audience and identify the needs of the public.

5.0 Design Guidelines

5.1 Design Guidelines

Government websites should be inclusive to all users, bearing in mind the diversity in technical knowledge and competency of the public. This section assists users to gain access to Government information and services in a more effective and efficient manner.

5.2 Website Structure

5.2.1 Develop a User-centric Structure for the Website

A website's structure is about organizing the website's content, information flow and category or subject hierarchy in such a way that users can logically navigate through the website with ease, track progress and determine their location within the website on any web page.

All websites should ensure that:

i. the user does not need to have an understanding of the internal structure of Government or particular Government Institutions in order to find information or services;
ii. visitors need to be able to quickly assess menu items on the website on each page. Menu items need to be properly labelled in a manner that ascertain information context.

5.3 Page Layout

5.3.1 Home Page

a. The home page must be informative, inviting, concise and easy to read.
b. It should provide sufficient information for visitors to recognize what is being communicated.
c. It must allow for easy navigation
d. It must avoid clutter in the form of distracting animations, unnecessary graphic elements, blinking or scrolling text.

5.3.2 Other Pages

Establish a visual identity and apply it consistently throughout the website. The branding of a website can be established by incorporating common design elements such as colours, logos, styles, etc., into every page. This presents a professional and consistent visual identity throughout the website as well as an important signpost that tells visitors where they are. Also, pages should be brief. Divide long

pages into multiple interlinked smaller pages with appropriate sub menus.

5.3.3 Navigation

5.3.3.1 Provide Consistent Navigational Links

a. The navigation system should be intuitive to help the public to easily locate information or services.
b. Links to the homepage and the search facility should be provided on every page. Links allow users to easily navigate from one area of the website to another.
c. The size, shape, position and function of important elements should remain consistent. Users should be able to navigate the entire website without using their browser's back button.
d. Navigation to websites on a different domain should be done on a new window. It is important to note that the new window should NOT be a popup of a differently sized window to prevent cluttering the users' screen

5.3.3.2 Use Navigational Links that are Easily Recognized

Many web navigation labels, such as *Home, About Us, What's New, Media Releases, Publications, Search, Contact Us, Useful Links, Website Map, Feedback* and *Help* are widely accepted terms. Unique and creative labels may look good, but can have a detrimental effect on website usability. Stick to plain English terms for navigation labels except where it is imperative to use unconventional terms.

5.3.4 Include a Website Specific Search Facility

Many people visiting a site are not interested in looking around a website. They want specific information quickly. Cater for the needs of this group by including a website specific search facility or link to one on every page. A link to the sitemap of the website should also be included at the footer of every page

5.3.5 Provide Access to the Nigerian Government Search Portal

The structure of Government can often confuse users when determining which institution's website is likely to contain the information they need. Providing a link to the Nigerian information portal http://nigeria.gov.ng.

5.3.6 Provide 'Bread Crumbs' on Every Page

At the top of each web page, provide a list of all levels between the home page and the current page, each of which is a link.
For example:
"Home > About Us > Our People > Director-General".
This breadcrumb approach provides context and allows the user to travel back up the hierarchy to any level without having to hit all the intermediate links.

5.3.7 Provide a Site Map to Aid Navigation

Site maps represent the structure of the website both textually and graphically in a single view. They provide an excellent overview of the website and allow for quick access to the major pages.

5.4 Hyperlinks

5.4.1 Create Labels that Accurately Describe the Destination of Links

Text links must be worded in a manner that reflects the destination of the link. This allows the user to quickly identify links of interest and also helps address accessibility and usability issues. Do not use meaningless labels such as 'Click Here' or 'Go'. For example, rather than 'click here to know more about us'.

5.4.2 Create Links that are Easily Recognized

All links, irrespective of whether they are presented as images, buttons or text, must be easily recognized. Appropriate visual cues should be adopted to clearly identify links.
Text links should be:

i. underlined or coloured;
ii. images that link to other pages should look like and act like buttons;
iii. mouseover effects such as background or foreground colour changes for text and images should be used to emphasize that the object is a link.

5.4.3 Clearly Separate Links that Occur Consecutively

Consecutive links are difficult to read and must be clearly separated.
For example:
About Us \ News and Events \ Publications.

5.4.4 Differentiate Visited Links from Unvisited Links

Web browsers, by default, display visited and unvisited links differently. Avoid developing websites that override this behaviour, making it impossible to differentiate visited links from unvisited links. A change of colour is most often used to differentiate between visited and unvisited links. It is widely accepted that blue is the colour that displays a link the user has not visited.

5.4.5 Evaluate the Appropriateness of Links to External Websites

When linking to other Government Institutions or private organizations, text around the link should make it clear to the user that they are about to leave the institution's website. It is strongly recommended that external websites be opened on new windows or tabs; the use of an icon signifying to the user that an external page will be opened may be employed.

Links must connect to valid pages that contain relevant data. A link to a website of a non-government organization may be perceived as an endorsement of that organization. Assess the implications of using these types of links carefully. Ensure there is no implicit endorsement or any commercial advantage except it doesn't contravene the Institutions' policy. It should also be made clear when linking to external websites that the information provided is the responsibility of that external source and not of the referring website.

5.5 Appearance

5.5.1 Screen Resolutions

Resolutions for Government websites must be fluid and adaptive. It must be designed to display properly on extra small devices, small devices, medium devices and large devices. Below is a resolution chart for width:

i. extra small devices (Mobile phones) **< 768px**;
ii. small devices (Tablets) **>= 768px**;
iii. medium devices (Basic sized computer screens) **>= 992px**;
iv. large devices (Large sized computer screens) **> 1200px**.

5.5.2 Fonts

Make text easy to read by using default or standard fonts. The display properties of text (typeface, size and colour of fonts) must be readable in both electronic and printed form. Not all fonts are supported or accessible by all users. Select standard font types (such as Arial,

Verdana, Times New Roman, etc.) or embed it using cascading style sheets referencing the font file. Use font sizes that make it easy to read the text on screen. Keep in mind that the user's browser determines how the text appears on screen. Limit fonts to one or two types and apply font styling consistently throughout the website.

5.5.3 Colours and Backgrounds

Use the selected colour scheme consistently. Select a suitable colour scheme and apply it consistently throughout the website. Use colours from the 216 colour browser safe palette. Ensure the colours used for text and graphics are legible on a variety of platforms and monitors by selecting them from the 216 colour browser safe palette. Use colours that contrast well on screen and on paper.

The contrast of text against the background must be sufficiently high to ensure it is legible on both screen and on paper. The "dark on light" approach should be adopted to improve the readability of information. Black text against a white background produces the best results. Avoid background textures or graphics. Avoid a textured or tiled background so as not to weigh down the page, making it slow to load. Use colours that accommodate people with a colour disability. The use of colour and how accessible it is to users is an issue that should not be overlooked in web design. It must be considered carefully as it can have an effect on the public's ability to use the website.

5.5.4 Images

Do not use images where it is unnecessary. Images can add life to a website, however, they can also be distracting and will slow download time. For image icons, use iconic fonts (e.g. fontawesome). Iconic fonts are better at reducing bandwidth real-estate; and since they can be styled, results in a more consistently branded website. Images should only be used when they add value to the content. The use of text, rather than images, should be considered for headings and website navigation. Images should be created in an appropriate format to minimize load time and maximize the display quality. Images should be compressed through the quality and size attributes where necessary. Commonly used images, such as those for website identity and navigation should be reused to decrease download time.
Note: images stored in the browser's cache will not need to be reloaded and will display faster.

5.6 Multimedia and Animation

5.6.1 Minimize the Use of Animation as it Slows the Loading of Pages

The use of animation can be an effective means for drawing attention to key aspects of a website. However, ensure it does not distract or irritate users or lead to long download times. Use animation only where appropriate, CSS animations is preferred over flash animations due to security and performance issues widely noticed on flash animations. File sizes of animated images should be kept small by limiting the number of frames-per-second used so as to reduce download time.

5.6.2 Provide Text Equivalents for Video and Audio Clips

Ensure the content of video and audio clips is accessible to all by providing text and/or, audio descriptions of video clips for the visually impaired or those accessing the information on slow connections; transcripts or at least a description of audio clips, for the hearing impaired or those who do not have access should be added.

5.6.3 Provide Download Details for Video and Audio Clips

Download information should be provided to help users determine whether they wish to access the video or audio clip. This includes the download and usage instructions, subject matter description, file size, and file format (MPEG, WAV, QuickTime, etc.). If a specific software programme is required, provide a link to enable the user download it. Where possible, use a detection script for any plug-in used. Minimize formats of multimedia used across the website. Choose streaming rather than forcing users to download the entire file.

5.7 Display

5.7.1 Design Applications for Standards not for Browsers

As many web based applications will continue to be developed and find their niche in the market, so will the range of web browsers. Given this, it is prudent to design web based applications for standards, not for browsers.

5.7.2 Maximize User Access

Maximize user access by providing alternate mechanisms for accessing web pages that rely on scripting languages or Java applets. Website functionality delivered through client side scripting (including Dynamic HTML using Javascript) or Java applets (e.g. visual effects, electronic forms, etc.) must be accessible to the widest possible audience. This may require the development of alternate facilities that ensure successful operation under different browsers. Special 'browser sniffers'

can be used to detect the browser in use and download alternative web page versions as appropriate.

5.7.3 Use Cascading Style Sheets (CSS) to Control Presentation

The use of CSS allows various styles to be defined and modified independent of the website content. Ensure consistency in presentation across the website and to aid web page development and maintenance. Style sheets should not be used in a manner detrimental to accessibility for browsers not supporting certain features.

5.7.4 Use Templates for Consistency

Web page templates can be used to maximize consistency and greatly reduce the time and effort required to create and maintain website content. Templates often contain calls to standard CSS and common header, footer, navigation and metadata elements.

5.7.5 Avoid the Use of Frames

Frames present a number of usability problems and should be avoided. Frames interfere with bookmarking, printing, indexing and retrieval by search engines, and using the browser's "back" button. Websites that use frames should provide a suitable non-framed alternative.

5.8 Forms

5.8.1 Provide Forms that are Easy to Understand and Complete

There are some basic principles that apply to form design, irrespective of whether the form is in electronic or hardcopy format. Forms should be:

i. Clearly documented to identify their purpose, who should use them, when they should be used, how to complete them, and where to submit them,
ii. Easy to complete by providing easy presentation, consistent layout and structure (including field labels), unambiguous wording, logical group of questions, and sufficient room for each response.

Other requirements for electronic forms to be completed and submitted over the internet are listed below:

i. Full disclosure of matters relating to the privacy and security of the submitted information must be made,
ii. Appropriate navigation facilities and indicators are to be provided,

iii. All field items should be arranged vertically (down the screen) to aid readability,
iv. Form pre-filling should be utilized wherever possible,
v. Errors resulting from incomplete or invalid information should be detected upon submission and immediately communicated to the user for correction. When an input error is detected and the user is returned to the form to correct it, retain all valid information already entered except passwords,
vi. The user should be provided with the opportunity to verify and edit the form prior to final submission,
vii. Upon submitting the form, the user should be issued with a printable electronic receipt notifying that the form has been accepted; and
viii. Ensure the user is provided with an option to print a completed copy of the electronic form.

5.8.2 Provide Alternatives to Electronic Forms

Electronic forms can be an effective means of capturing information. Suitable alternatives to electronic forms should be provided *(except it contradicts a Government policy to do so)*. This may include the provision of:

i. downloadable forms in Rich Text Format (RTF) and PDF format, which can be completed offline and sent via email,
ii. a telephone number, and monitored email contact details for requesting a hardcopy, further information, or assistance.

5.9 Mailing Lists

Where the websites provides for a mailing list the following shall apply

5.9.1 Make it Easy for Users to Subscribe and Unsubscribe to Mailing Lists

All messages sent to the mailing list must explain how to unsubscribe and a link to do so on the footer of the email. When a user unsubscribes, an acknowledgement message should be sent that confirms that they have been removed from the list.

5.9.2 Minimize the Size of Emails sent to Mailing Lists

Keep emails to subscribers succinct. The email text should be limited to brief summaries and provide links, where necessary, to more extensive contents or downloads on the website. Avoid including file attachments, as they may be rejected by the user's security systems. For branding purposes emails to users should be HTML formatted.

5.9.3 Be Consistent

Email formats should be consistent.

5.10 Discussion Groups

When setting up a discussion group, a number of important issues need to be determined:

i. The name and purpose of the discussion group; choose a name that is descriptive and relatively short. The purpose of the discussion group should closely define the subject boundaries for messages,
ii. The technical rules about how to subscribe, unsubscribe and details on how to get help should be made available,
iii. 'Netiquette' or subscriber behaviour rules should be made available,
iv. The need for disclaimers, copyright and privacy statements,
v. What type of discussion group to operate (i.e. open or closed, moderated or not moderated and how secure),
vi. It is MANDATORY that discussion forums be moderated to prevent the automatic publishing of inappropriate material on Government websites and enable an administrator to create, edit and delete content and any discussion forum. It is also important that suitable administrative and resourcing arrangements are in place to support discussion forums.

5.11 Downloads and Plugins

5.11.1 Provide Information that will Help Users Determine whether they want to Access Downloadable Materials

Downloading materials from the internet can be an expensive and time- consuming exercise. Inform users about downloadable materials by providing information concerning the subject matter, download and installation instructions, file format, file size and running time for video or audio clips.

5.11.2 Create Quick Loading Pages by Minimizing File Sizes

The total size of a web page (including code, images and scripts) should be kept to a minimum to ensure acceptable download times and sizes for all users.

5.11.3 Ensure all Downloadable Material is Virus Free

Prior to making downloadable materials available it must be checked and cleared of virus.

5.12 Directory Structure and File Naming

Employ best practice conventions for file and directory naming. To enhance portability of websites and reduce the risk of broken links, where applicable adopt the following file and directory naming conventions:

i. Use lower case for the file and directory names,
ii. Ensure file and directory names are continuous, i.e. no spaces, but underscore (_) or hyphens (-) are acceptable,
iii. Limit file and directory names to fewer than 20 characters,
iv. Specify the correct file name extensions. For example, htm, html, gif, jpg, png, rtf, doc(x), xls(x), pdf.

5.13 Authoring, Error Messages and Printing

5.13.1 Authoring through a Web Content Management System

A web content management system is a software that provides website authoring, collaboration, publishing and administrative tools designed to allow users with little or no knowledge of web programming languages or mark-up languages to create and manage website content. If such system is in place, it is important to apply the following principles:

i. Hierarchy of approval; who approves content, how and at what stage,
ii. Tasks applicable to each role in the hierarchy; creator, reviewer, approver, editor, website administrator,
iii. The authoring role in relation to different types of events, i.e. add new content, review and amend content, remove content,
iv. Avoid conflicting information on the website by being aware of possible content or concept duplication by other authors,
v. The database and folder structure of the content management system should be backed up once a week,
vi. All recommended security settings must be in place to mitigate hacking of the website,
vii. Super Administrative passwords and roles must be configured for the Head of ICT within the Government Institution and no more than two other persons within the Institution.

viii. In a case of Staff transfer, resignation, termination or retirement all roles and privileges must be revoked as part of the HR checklist for such staff

5.13.2 Clear and Informative Error Messages

Government Institutions shall:

i. Avoid errors being generated in the first place through regular website maintenance,
ii. Never remove or move a page without correcting the link from its original location,
iii. In addition to software tools are commonly used to assist with the regular checking for broken links also check for broken links manually,
iv. Create error messages which provide a clear explanation (free of technical terms).

5.13.3 Printing

Enable users to obtain hardcopies of documents split across multiple web pages. Where possible provide alternative versions that may be downloaded or accessed through a single continuous web page. Check that web pages print properly. Most printers print less characters across the page than are displayed on an 800x600 screen (570 pixels is a good printing width).

6.0 Development

6.1 Steps in Constructing Government Websites

The following steps shall be adopted by Government Institutions for the construction of government websites.

6.1.1 Definition of Objectives and Business Analysis

Define from inception the desired outcomes for the public, source of funding for website maintenance and the quality that is expected of the design.

6.1.2 Requirements Definition

Declare clearly what is required to achieve the objectives; who will be served, by who and what resources will be required and at what time?

6.2.3 Planning Specifications

Decide how the needs of the website users will be met; specify the structure of the website project, project team, management, finance, marketing, technical specification, functional and non-functional specification and domain registration.

6.2.4 Development

The development phase will include the following:

i. Selecting the implementing infrastructure,
ii. Procurement,
iii. Establishing the design elements and navigations,
iv. Developing content.

6.2.5 Design and Implementation

The design stage shall deal with the development of the User Interface (UI). The creation of the various UI elements to be used in the website must conform to the recommendations stated in the Design Section of this document.

The website code (HTML, CSS, JavaScript, etc.) should be written in a manner which conforms to industry standards for best practices to ensure code readability and maintainability. Same principle should be followed if developing the website through a programming language (PHP, Python, Ruby, Java e.t.c.) or framework (Django, Ruby on Rails, Laravel, Flask e.t.c.).

6.2.6 Testing

Testing must be carried out in order to ensure the final product satisfies its business case. The following tests constitute the minimum requirements for ensuring the technical integrity of a government website and they form the minimum requirement for the testing phase;

i. Functionality Testing
ii. Usability Testing
iii. Interface testing
iv. Compatibility Testing
v. Performance Testing
vi. Security Testing

A website/web application MUST undergo a security audit that conforms to the Open Web Application Security Project (OWASP) Testing Guide prior to hosting. The report MUST reflect a Zero 0 Number of Alerts for High and Medium Risk Levels.

6.2.7 Maintenance, Quality Control and Review

The following activities must be carried out for maintenance and quality control of a website:

i. Regular checks for broken links,
ii. Website statistics,
iii. Email monitoring,
iv. Disaster recovery viability,
v. Content management training,
vi. Project evaluation and review,
vii. Maintenance and renewal for hosting.

7.0 Web Security & Privacy

7.1 General Information

Government Institutions shall put measures and controls to protect their web resources to assure the Confidentiality, Integrity and Availability of information. Government Institutions shall ensure that information contained on their websites are safe and securely stored, retrievable and removable.

7.2 Guidelines for Web Security and Privacy

The following guidelines shall be adopted for securing Government Websites as well as for ensuring personal privacy on the Web:

i. In securing web content, all Government Institutions shall develop website security plans with respect to the National IT Policy. Government Institutions shall ensure that users are alerted of potential risks and how to avoid them when accessing the website.
ii. Government websites shall include a standard privacy policy statement that stipulates:
    a. how information collected is used
    b. circumstances where information can be disclosed to a third party
    c. if the information is accessible by the public
iii. Government Institutions shall regularly conduct security threat and risk assessments on their websites as well as create and regularly review a security plan that describes the necessary security mechanisms and procedures.
iv. Where Government Institutions solicit or collect information from users through electronic forms or email, they shall ensure that this information is securely transmitted and stored by taking appropriate measures such as data encryption.
v. Where Government Institutions need to transmit information to users, they shall ensure that the information is protected through appropriate technologies (e.g. SSL). Reasonable care shall be taken to protect the personal information held by a Government Institution from misuse, loss, unauthorized access, modification and disclosure.
vi. Where necessary, user registration for access and use of services such as access to Government databases shall be enforced.

7.3 Hosting and Web Services

The following guidelines shall be followed when hosting Government Website and Services:

i. All Government websites and their domains shall be hosted in Nigeria (*Refer to the Regulatory Guidelines for Nigerian Content Development in ICT - 2013*).
ii. No government Website shall be hosted outside Nigeria unless on the Written Authorization obtained from NITDA.
iii. Government Web hosting shall aim to ensure the high availability of Websites, Databases, Applications and Services.
iv. Government web hosting shall provide for secure remote access through secure channels
v. Government Institutions shall manage their web hosted applications through a secure management tool that provides control, flexibility and reliability.
vi. There shall be regular back-ups of all hosted content for the purpose of ensuring business continuity in case of failure.
vii. Government Institutions shall also develop a comprehensive business continuity and disaster recovery plan.
viii. Government Institutions shall ensure that Web security strategies are put in place.
ix. Government Institutions shall implement real-time event log monitoring for critical security incidents and periodic analysis.
x. Mechanisms to monitor security-relevant policies (e.g., authentication, authorization, etc.), activity (e.g., privileged user activity) and applications (e.g., IDS, IPS, firewall, etc.) in real time should also be put in place.

7.3.1 Hosting Service Requirements

Government Institutions MUST execute a Service Level Agreement (SLA) and Non-Disclosure Agreement (NDA) designed to ensure Confidentiality, Integrity and Availability of all government web applications hosted by Hosting Service Provider (HSP).

Government websites MUST be accessible to the public in a fast and secure manner on a 24-hour basis and on all days of the week. It is important that the Web Hosting Service Provider (HSP) for a Government Institution be chosen with extreme caution and care and

the following shall form the minimum requirements:

i. Application switches shall ensure that appropriate levels of resources are available to cater for seasonal loading peaks.
ii. A secure and private connection from the internal network shall be provided for management access.
iii. The HSP MUST possess state-of-art multi-tier security infrastructure both at physical and network level as well as security policies to ensure the best possible security to Government websites.
iv. The Web Hosting Service Provider MUST have in place a firewall and intrusion prevention systems to make the website more secure.
v. The Web Hosting Service Provider MUST have a redundant server to ensure fastest restoration of the website in the event of any unforeseen hardware/software failure.
vi. The HSP MUST perform regular backups of the websites.
vii. It is mandatory to conduct a mock test to proof workability of the disaster recovery system.
viii. The HSP MUST have a Disaster Recovery (DR) Centre in a geographically distant location of no less than 15 kilometers and a well drafted DR plan for fast restoration of the services during any disaster.
ix. The HSP shall provide the facility of staging infrastructure in order to facilitate the testing of the Government website before hosting.
x. HSP should provide web server statistics required for performance evaluation on a regular basis. If possible, online access to the traffic analysis should be provided so that Government Institutions can access the traffic analysis at any point in time.
xi. HSPs MUST make provision for alternative energy sources to ensure service availability 24 hours every day of the week and a helpdesk with technical support to the Government Institutions all year round. This provision is mandatory in the Service Level Agreement

7.3.2 Security of Government Institution's Web Servers

Government Institutions shall implement appropriate security management practices and controls when maintaining and operating Web servers.

To ensure the security of Government Institutions Web server(s) including the supporting network infrastructure, the following practices shall be implemented:

i. Information System Security Policy
ii. Configuration/change control and management
iii. Risk assessment and management
iv. Standardized software configurations that satisfy the National Information Security Framework of the National IT Policy
v. Conduct regular Security awareness and training for Government Institutions' staff
vi. Develop and implement contingencies for operation and disaster recovery for Web Servers.

In deploying Government Institutions Web Server(s) the following considerations shall be taken into account:

a. Government Institutions shall ensure that server operating systems are deployed, configured, and managed to meet the security requirements of the Government Institutions.
b. In securing Web Server Operating Systems, Government Institutions through their respective IT Units shall:
    i. In a timely manner patch and upgrade the server OS when made available by the OEMs.
    ii. Disable unnecessary services, directory listings and applications.
    iii. Configure operating system user authentication.
    iv. Configure Web server resource controls.
    v. Perform security testing of the operating system.

7.3.3 Security of Web Content

Government Institutions shall ensure appropriate steps are taken to protect Web content from unauthorized access or modification.

In ensuring the security of Web Content, Government Institutions shall:

i. Commit to continuous process of maintaining the security of Web Servers to ensure continued security.
ii. Use authentication and cryptographic technologies as appropriate to protect certain types of sensitive data with differing access privileges. It is recommended that SSL be used for any cryptographic implementation
iii. Limit the use of interactive elements on web pages as these may introduce web-related vulnerabilities since they involve dynamic execution of codes

iv. The web server should be backed up periodically
v. Establish and follow procedures for data recovery in case of compromise
vi. Define complete Web content access matrix that identifies which folders and files within the Web server document directory are restricted and which are accessible
vii. Use host-based Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS)
Protect each database server from command injection attacks.

8.0 ACCESSIBLITY

Incorporate common design elements such as colours, signposts, logos, styles into every webpage in a professional and consistent manner to improve and enhance user experience.

8.1 Accessibility and Promotion

Government Websites shall provide equal access to information and functionality to all users.

For Web accessibility the Government Institutions shall:

i. Adopt the Web Content Accessibility Guidelines (WCAG) developed by W3C. The guidelines cover a wide range of recommendations for making Web Content more accessible to a wider range of users including those with disabilities (visually impaired, deafness, hearing disabilities, cognitive limitations, limited movement, speech difficulties, photosensitivity, etc.),
ii. Ensure that webpages do not contain any blinking, scrolling text, or flashing objects.
iii. Ensure that accessibility applets, plug-ins, downloads and applications that are required to interpret page content meet the requirements and are tested to ensure that they can be used by assistive technologies.
iv. Avoid the use of uncommon media plug-ins which may redirect the users to other websites to download plug-ins.

8.2 Metadata

8.2.1 Definition

Metadata is structured data that describes the characteristics of a website and the webpages. Metadata properties help search engines' bot crawl through the website selecting terms that will appear on search results.

8.2.2 General Guidelines for use of Metadata

The following guidelines shall be considered in describing, managing and preserving Web based information:

i. All Government Institutions shall use metadata to describe their web based information to improve the visibility and discoverability of those resources via web based search facilities.
ii. All Government Institutions shall use Metadata for preserving and managing electronic records and ensuring their continued accessibility over time.
iii. All Government Institutions are required to apply the generic metatags; "keywords" and "description" which are indexed by the majority of commercial search engines. Government Institutions are encouraged to use as many additional metadata elements as are necessary to enhance their resource description and maximize discovery.

8.3 Search Engine Optimization (SEO)

To further improve or enhance visibility of Government Websites using Search engines, the following guidelines shall be applied:

i. Usable search results shall be incorporated on the Websites. Avoid using confusing search results by providing precise information that matches the expectations of the users.
ii. All Government Institutions shall ensure that search engines search the entire website including pdf files, or clearly communicate which part of the Website will be searched. It is important to provide facility that narrows the scope of searches from a large search result by selecting relevant options.
iii. Ensure the image files are labelled properly to be discoverable.
iv. Ensure image elements have alternate names for to improve search and to aid accessibility.
v. Ensure that searches are not case sensitive. Disregard case sensitivity on the search when entered as search terms.
vi. Provide search options on every webpage that enables the user to filter search.

10.0 Legal

The following legal aspects shall be considered in developing and managing websites.

10.1 Website Terms and Conditions

All Government Institutions shall ensure that their Terms and Conditions shall address the following aspects:

i. Website ownership details
ii. Usage policy of the posted content on the Website
iii. Legal considerations on the usage of the Website
iv. Responsibility towards hyperlinked sites

Content of another Government website is not out rightly disclaimed but rather indicate the ownership of a particular piece of content as well as refer users to appropriate support channels where further enquiries and feedback may be made. Clarity is provided on whether the information available on the website may be construed as a statement of law to be used for any legal purposes or not.

Websites should set out the terms and conditions of use on which the content and services are provided to users. The terms and conditions should cover all aspects of the scope and operation of the website. They should, at the very least, be available from the website's home page, but preferably accessible from every page on the web footer.

10.1.1 Content Hyperlinking

Government Institutions should ensure a clear and concise hyperlinking policy is adopted in order to minimize the risk of liability.

i. The hyperlinking policy enumerating the detailed criteria and guidelines with respect to hyperlinks with other sites may be made available under the common heading of ''*hyperlinking policy*'' and should be part of the terms and conditions.
ii. Clear indications should be given to visitors when leaving the Government Institutions website to a non-government website. Considerably, there could be a difference in the security domains of two linked websites. The visitors should be notified of such difference through a hyperlink while entering another one.

A link to a website of a non-government organization may be perceived as an endorsement of that organization. Government institutions should therefore assess the implications of using these links

and should ensure that there is no implicit endorsement or any commercial advantage given. Government Institutions shall:

i. Links should open as externally linked pages in a new browser window.
ii. It should also be made clear when linking to external websites that the information provided is the responsibility of that external source and not of the referring website.
iii. Check the conditions of use and copyright statements of the website before any link is created. If a website specifically states that it does not permit deep linking or any other type of linking, then the practice should under no circumstances be undertaken.
iv. If the administrator of a website alleges infringement of copyright or other rights as a result of the method used by a Government Institution to create a link, it must be rectified immediately.
v. If it becomes clear that a linked website includes infringing material, the link should be deleted immediately.

10.2 Content Copyright

All Government Institutions shall ensure that:

i. Any information or documents made available on a Government Institution's website should be supported with proper copyright policy explaining the terms and conditions of their usage and reference by others.
ii. Government Institutions should also be careful towards publishing any information having a third party copyright. All Government Institutions must follow proper procedure to obtain the permission, prior to publishing such information on their websites.
iii. If any publication or report is reproduced on any Government Institution's website whether in part or in full, the title of the document or report including the name of the concerned department and year of publication must be referenced.

10.3 Other Legal Liability Issues

10.3.1 Domain Names

All government websites are mandated to be on the "***.gov.ng"*** top level domain (TLD).

10.3.2 Defamation

Anything on a website that could be construed as having the potential to injure a person or organization's reputation should be scrutinized thoroughly and legal advice should be sought accordingly. Where

there is any doubt at all, it may be best to remove the alleged offending material from the website until a properly informed decision can be reached.

10.3.3 Penalty

Any breach of these Guidelines is a breach of the NITDA Act 2007 and shall be punished in accordance with the provisions of the Act.

10.4 Privacy Policy

Government Institutions shall:

i. Exercise diligence when collecting personal details/information about the visitors to the Website.
ii. Incorporate prominently displayed Privacy Statement clearly stating the purpose for which information is being collected where the Government Institution seeks to or collects personal information from visitors through their website.
iii. Adopt a secured means of collecting high risk personal information from the public such as credit card/bank etc.

11.0 Website Management

Government Institutions shall undertake the following task:

i. Setting the objective of the websites,
ii. Ensuring that the website is appropriately resourced,
iii. The delivery of information resources and services on the website,
iv. Conducting quality reviews to monitor the quality of information and services offered on the websites,
v. Conducting reviews to monitor the usability of the websites,
vi. Identifying and refinements of service objectives, and new initiatives to deliver these objectives,
vii. Commissioning of websites and the overall management of the institution's website.

For smaller government institutions or web initiatives it may be appropriate to have these responsibilities vested in one officer rather than in a management group. Government institutions may also deem it appropriate to use a management group for major website initiatives, and vest editorial responsibility in one or two officers for ongoing updates to the website.

11.1 Operational Plan for Managing Websites

The operational plan shall include the development of and regular review of all plans associated with a website including online service plans, financial plans, risk management plans, information management plans and marketing plans where necessary.
The plan should include responsibility for review as well as associated timeliness for conducting and finalizing the process.

11.1.1 Reviewing the Plans

Regular review of the plans is required to:

i. Compare expected benefits with actual outcomes,
ii. Make contingency plans for unforeseen events (e.g. additional costs, budget reviews, staff movement, benefits),
iii. Identify charges required to enhance returns,
iv. Implement changes to content.

Reviews of the plans address a variety of key issues such as:

i. Ongoing monitoring of activity on the website,
ii. Modifying the website to adapt to emerging customer and technology needs,
iii. Monitoring and possible modification of budgets,

iv. Modifying and expanding associated information storage and retrieval systems,
v. Updating hardware and software,
vi. Meeting new staff training requirements (e.g. security issues, 'authoring', and
vii. Taking advantage of new marketing opportunities for the website.

Apart from maintaining and improving the viability of the site, the review process serves to highlight potential problems and identifies any changes required to better meet the needs of the public and the institution.

11.2 Monitoring and Evaluating the Website

11.2.1 Website Feedback

Government Institutions shall provide a feedback mechanism to provide the public with the opportunity to send comments to the website administrators and authors on information published.
An officer should be assigned to review comments and respond within 72 hours from receipt.

11.2.2 Self-Audits

A proactive approach to web management is to undertake self-audits. This internal review should involve:

i. Monitoring reported problems and customer queries over a period of time, with the view that these should decrease if appropriate corrective action is taken,
ii. Monitoring website reliability,
iii. Monitoring the accuracy, consistency and completeness of information, offered on the website,
iv. Reviewing the website for its adherence to established policies and guidelines.

11.3 Website Maintenance

11.3.1 Information Integrity

The information management plan should include various measures for maintaining information integrity, such as:

i. Undertaking regular checks on the accuracy of the information.
ii. Regularly check that all information posted on the website are updated frequently.

iii. Removing sections that are no longer useful, with appropriate consideration for archiving and record-keeping regulations. However, never remove or move a page without providing a link from its original location to a page where the information is now located.
iv. Checking links to other websites regularly to ensure that the link is still 'alive' and that content of the website is still appropriate. It is advised that programs for checking broken link is employed, however, external links should also be checked manually.
v. Ensuring the website delivers on any promises for new information or services to the public.

11.3.2 Decommissioning Websites

Websites should be regularly reviewed to ensure that they are still relevant and should be retired where the website:

i. Does not serve a specific function or purpose of Government,
ii. Was developed for a particular project or strategy that is no longer relevant or current,
iii. Was launched as part of a Government sponsored campaign that has come to an end. Particularly, where non-essential and website traffic statistics indicate that the website is not being utilized.

When decommissioning websites, consideration should be given to archiving the content appropriately.