Mobile Accessibility Guidelines

1. Perceivable
    a. Small Screen Size

    Small screen size is one of the major limiting factors in case of mobile applications. Go for a native mobile application which is able to make use of all features of both the device and the OS.

    b. Zoom/Magnification

    Mobile devices have built in features for text resizing and zooming, ensure that the application is able to respond to native magnification and text resizing gestures, except for captions and images of text should be resizable without assistive technology up to 200 percent without loss of content or functionality. Ensure that the application is not blocking this feature.

    c. Contrast

    Good color contrast not only improves user experience in lower specification devices, it also is easier on the eye in a brightly lit environment. It also provides assistance to visually challenged users. The following should be adopted for all texts except decorative texts and exceptionally large texts.

        i. Contrast (Minimum) (Level AA) which requires a contrast ratio of at least 4.5:1
        ii. Contrast (Enhanced) (Level AAA) which requires a contrast ratio of at least 7:1.

    d. Color

    It becomes difficult to distinguish the colors when the mobile devices are used in bright sunlight. Senior citizens and visually impaired also find it difficult to understand color coding. In addition to these assistive tools such as screen readers are not able to detect colors.

    Under no circumstances colors should be used as the only visual means of conveying information, indicating an action, prompting a response, or distinguishing a visual element.

2. Operability
    a. Keyboard Control for Touch screen Devices

    Most of the mobile operating systems include keyboard interfaces, allowing mobile devices to be operated by external physical keyboards (e.g. keyboards connected via Bluetooth, USB On-The-Go) or alternative on-screen keyboards (e.g. scanning on-screen keyboards). Support for external keyboards benefits persons with disabilities.apps must be tested with hardware keyboards also

b. Touch Target Size and Spacing

Appropriately sized touch targets will provide ease of use to all users including users with disabilities. All touch targets should be between 8X8mm and 10X10mm.

Touch targets should have some inactive area (minimum 1 pixel) in between and should not overlap with each other.

c. Touch screen and device Manipulation Gestures

Complicated touch screen gestures provide a good user experience for the users however it may be difficult to simulate complicated gestures for person with disabilities. Always use simple gestures even the platform has support for complicated ones. Avoid gestures that require 3 or more fingers to interact with UI elements

Use of device manipulation gestures such as tilting, shaking should be discouraged, if required always provide alternative methods for the same action.

d. Non text content such as Images, buttons or icons

People using screen readers are often vision impaired and unable to perceive non-text content. Providing a brief alternative that the screen reader speaks conveys the same meaning or purpose for non text content.

It is also suggested that decorative images should be hidden from screen readers.

e. Alternatives for audio and visual content

Provide captions for audio content and subtitles/transcripts for video content that is accompanied by audio

f. Placing buttons where they are easy to access

When designing applications many developers attempt to optimize use with one hand. This can benefit people with disabilities who may only have one hand available; however, developers should also consider that an easy-to-use button placement for some users might cause difficulties for others (e.g. left- vs. right-handed use, assumptions about thumb range of motion).

g. Ordering of elements

Both actionable and static content must be navigable in a meaningful sequence. The users using assistive technologies will be able to follow the flow in a meaningful way.

h. Focus

   Ensure that all interactive elements receive focus from assistive technologies using platform specific methods.

   If using a keyboard or other non-pointer input, user focus must be allowed to progress and not get stuck at a particular element.

i. Consistent Labeling

   Consistent and meaningful labeling will help all the users in interacting with the application; it will also provide meaningful input to screen readers. Application language should also be clearly indicated in each page in case of multilingual applications.

   In addition to above all form controls, such as text inputs, check boxes, select lists, or buttons, must each have a unique label.

j. Flicker

   Flickering may be annoying to certain set of users. Content must not visibly or intentionally flicker or flash more than three times in any one-second period

3. Understandable

   a. Changing Screen Orientation (Portrait/Landscape)

      Developers should try to support both orientations. If it is not possible to support both orientations, it should be ensured that it is easy for all users to change the orientation to return to a point at which their device orientation is supported. Changes in orientation must be programmatically exposed to ensure detection by assistive technology such as screen readers.

   b. Consistent Layout

      Mobile application with consistent layout in sync with the native platform will help the users in predicting where to find the relevant information and how to interact with the application.

      Do not change the functionality of buttons such as back button and home. Ensure that the applications follow the pattern of the native platform. Mobile development platforms such as Android and iOS have strict design guidelines, and users familiar with screen layout will always prefer applications which stick to native look and feel.

      If possible provide multiple methods to access the content such as tap on the screen or a swipe gesture.

c. Positioning important page elements before the page scroll

   The small screen size on many mobile devices limits the amount of content that can be displayed without scrolling. Important information should be positioned so that it is visible without requiring scrolling. It can assist users with low vision and users with cognitive impairments.

d. Notifications and Error Messages

   Notifications are meant to inform and guide users. They can be error messages, alerts, instructions, and changes of state, responding to an interaction or a range of other cues. Use operating system alerts or inline messages. Ensure that the notifications are audible and can be read by screen readers. Give preference to operating system alerts as they are easier to understand. Custom made notifications should be clear and precise.

e. Grouping operable elements that perform the same action

   Properly grouped elements help all users understand the relationships between various controls and make the application easier to use. For users of assistive technology, this can mean fewer steps and reduced complexity.

f. Provide clear indication that elements are actionable

   Users should be able to identify whether the content is static or actionable. Use platform specific buttons and navigation control designs including swipe areas clearly indicating the functions. Actionable elements should also be able to provide information to assistive technologies.

   When focused, all actionable and focusable elements must have a visible state change.

4. Robust

   a. Set the virtual keyboard to the type of data entry required

      On mobile devices it is possible to customize standard keyboard and also install additional custom keyboards. Some mobile devices also provide different virtual keyboards depending on the type of data entry. Setting the type of keyboard as per the data entry required prevents errors and ensures formats are correct.

      Ensure that the appropriate keyboard is invoked by the app depending on the type of field or the data that needs to be provided by the user. For example, the appropriate on--screen keyboard must be invoked for normal text, numerical data, email address or web address.

b. Provide easy methods for data entry

Some users will find it difficult to use conventional data entry methods such as touch screen. Ensure that alternative data entry and navigation methods such as Braille keyboard or display, also work with the applications.

In addition to this do not automatically change focus in the form, if a user is entering data and the focus shifts automatically, the user would find it difficult to enter data. Focus must be changed only when the user activates a UI element that is designated for confirming an action such as the Submit button.

c. Support the characteristic properties of the platform

Mobile devices provide many features to help users with disabilities to interact with content. These include platform characteristics such as zoom, larger fonts, grayscale, invert colors, voice commands and captions. Although support for such features is device dependent, application should be reviewed for all the accessibility options in the device settings and the developer should ensure that each accessibility feature behaves as intended.

Also ensure that the app designers follow platform specific design guidelines.

For Apple : https://developer.apple.com/ios/human-interface-guidelines/overview/design-principles/

For Android : https://developer.android.com/design/index.html

d. App size and storage

Users are reluctant to install and use apps which are large in size as mobile have limited storage. Ensure that the app is small to encourage installs and retentions.

e. Slow (2G) and usable data connections

Applications may be used in areas where network connectivity is erratic or slow. Ensure that the application is able to perform bare minimum functionality in absence of network connectivity. The users should be appropriately informed. Also ensure that the app uses network in an efficient and optimized manner.

For network management on an Android device go through https://developer.android.com/training/basics/network-ops/managing.html.

f. Users may not be able charge the mobiles frequently hence apps with heavy battery usage are uninstalled immediately. Avoid battery draining features. Best practices for optimizing battery life at https://developer.android.com/training/monitoring-device-state/index.html.

g. Before uploading the app on the play store ensure that it looks good on variety of screen sizes. Also ensure that the app runs of all popular versions of the target platform.

h. In order to make the app's Play store listing compelling, have a unique app icon, attention-grabbing images, video of app in action and crisp short description . Check the following links.

   Andriod : https://developer.android.com/distribute/best-practices/launch/store-listing.html
   iOS : https://developer.apple.com/app-store/insights/

i. App Promotion
   To increase awareness about the app follow the best practice at
   Google Play Store : https://developer.android.com/distribute/best-practices/index.html

j. User Feedback is an important source for suggestions and improvements. Hence keep a constant watch on app feedback and reviews at the platform specific stores.
   Google Play Store : https://support.google.com/googleplay/#topic=3364260

CONTENT

1. Splash screen of the app should clearly indicate the name of app, logo and Ministry/ Department Name and address.
2. Avoid using Logo, App Name etc on each page, so that due importance can be given to the app content.
3. Always ensure that the navigation menu or the main menu of the app has the following elements

   a. Clear instructions on using the app.

b. Have an “about <name of the app>” section in the app’s main navigation menu giving details about the version/build of the app and various other information such as contact information, ownership details , copyright notice , terms of use, privacy statement etc.

Security

1. Check your app against the mobile app security checklist at https://www.owasp.org/images/1/1b/Mobile_App_Security_Checklist_0.9.3.xlsx
2. Get your Mobile app and APIs security audited by Cert-in empanelled vendors.
3. Follow platform specific Security best practices.
   Android : https://developer.android.com/training/articles/security-tips.html
   iOS : https://developer.apple.com/security/
4. Use only HTTPS to access APIs

API and App Hosting

Mobile APIs

Security Audited APIs should be hosted in highly secure data centers equipped with firewalls and other security features.

1. Ensure that the hosting datacenter is able to provide 24X7 accesses to APIs and backend databases.
2. Configure appropriate disaster recovery site at different geographical location to avoid disruption of service in case of natural or manmade disasters.
3. API hosting service provider should also provide technical support and help to the owner of the application.
4. App developers should build adequate security measures in the API to detect and discourage unauthorized use of the APIs.

App hosting

Apps are invariably hosted on the play stores of the target platform which have their own policies and guidelines.

1. Play stores are a public platforms and any user is allowed to upload app after paying a nominal fees to become a registered user. However for better visibility and access

ensure that the app is uploaded through the official account of the API hosting service provider.

2. Ensure compliance to target platforms policies
   a. Android : https://play.google.com/about/developer-content-policy/#!?modal_active=none
   b. iOS : https://developer.apple.com/app-store/review/guidelines/

Contingency Management Plan & Disaster Recovery Process

Same as Website for of APIs and backend databases.

Mobile applications are hosted on Play stores of the respective vendors having their own Contingency Management Plan & Disaster Recovery Process

Policies

Privacy Policy for Mobile Application

Privacy policy should be a carefully written document clearly stating purpose of collecting the information if any through the app. It should also clearly state the mobile resources app is liable to use such as contact list , SMS, Folders, etc.

Sample privacy Policy

This privacy policy governs your use of the <*Name of App*> mobile application that is hosted at NIC's e-Gov Mobile App Account in Google Play Store. The contents published on these Applications were provided by the concerned Ministries/Departments of Government of India or the allied government establishment. This information provided through these applications may not have any legal sanctity and are for general reference only, unless otherwise specified. However, every effort has been made to provide accurate and reliable information through these applications. Users are advised to verify the correctness of the facts published here from the concerned authorities. National Informatics Centre will not be responsible for the accuracy and correctness of the contents available in the application.

User Provided Information

The Applications may obtain the information you provide when you download and register the Application. Registration is optional. However, please keep in mind that you may not be able to use some of the features offered by an Application unless you register.

When you register and use the Application, you generally provide (a) your name, email address, age, user name, password and other registration information; (b) download or use applications from us; (c) information you provide when you contact us for help; (d) credit card information for use of the service, and; (e) information you enter into our system when using the Application, such as contact information and other details.

The information you provided may be used to contact you from time to time to provide you with important information and required notices.

Automatically Collected Information

In addition, the Application may collect certain information automatically, including, but not limited to, the type of mobile device you use, your mobile devices unique device ID, the IP address of your mobile device, your mobile operating system, the type of mobile Internet browsers you use, and information about the way you use the Application.

When you visit the mobile application, it may use GPS technology (or other similar technology) to determine your current location in order to determine the city you are located within and display a location map. The location information may be sent to authorities for taking necessary actions and making policy decisions..

If you do not want the app to use your location for the purposes set forth above, you should turn off the location services for the mobile application located in your account settings or in your mobile phone settings and/or within the mobile application. However, if the service provided by the Application requires the location services using GPS technology, such services offered by the application will not be available for you.

We may disclose User provided and Automatically Collected Information:

- as required by law, such as to comply with a subpoena, or similar legal process;
- when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, investigate fraud, or respond to a government request;
- with our trusted service providers who work on our behalf, do not have an independent use of the information we disclose to them, and have agreed to adhere to the rules set forth in this privacy statement.

You can stop all collection of information by the Application easily by uninstalling the Application. You may use the standard uninstall processes as may be available as part of your mobile device or via the mobile application marketplace or network.

Data Retention Policy, Managing Your Information

We will retain User provided data for as long as you use the Application and for a reasonable time thereafter. We will retain Automatically Collected information also for a reasonable period of time depending on the nature of application and thereafter may store it in aggregate. Please note that some or all of the User Provided Data may be required in order for the Application to function properly.

Misuse by Non Targeted Users

All mobile apps are meant for use by the targeted audience only. Misuse by non-targeted users should be prevented by owner of the mobile.

Security

We are concerned about safeguarding the confidentiality of your information. We provide physical, electronic, and procedural safeguards to protect information we process and maintain. For example, we limit access to this information to authorized employees and contractors who need to know that information in order to operate, develop or improve our Application. Please be aware that, although we endeavour to provide reasonable security for information we process and maintain, no security system can prevent all potential security breaches.

Changes

This Privacy Policy may be updated from time to time for any reason. We will notify you of any changes to our Privacy Policy by posting the new Privacy Policy here . You are advised to consult this Privacy Policy regularly for any changes, as continued use is deemed approval of all changes. You can check the history of this policy by clicking here.

Your Consent

By using the Application, you are consenting to our processing of your information as set forth in this Privacy Policy now and as amended by us.

Contact us

If you have any questions regarding privacy while using the Application, or have questions about our practices, please contact us via email at <e-mail_id>[at]gov[dot]in.

IPR and Copyright

As mobile applications are hosted on Play stores which are essentially a public platform IPR and copyright have an extremely important role to play. An appropriate copyright notice can help deter infringement/plagiarism of the app as well as associated APIs.

Copyright statements can also be uploaded on the play stores along with the app clearly indicating the ownership.

Before launching an app get the app Name and logo protected through IPR (http://ipindia.gov.in/index.htm).

Ministries/Departments owning the app should identify competent authority to report/ escalate issues related to copyright infringement and misuse of APIs.
Google Play store : https://support.google.com//legal/troubleshooter/1114905
Apple App Store : https://www.apple.com/legal/internet-services/itunes/appstorenotices/#?lang=en

Sample Copyright policy

Name Logo and design of the app is subject to copyright protection. The content may be viewed/downloaded without requiring any specific prior permission. Any other proposed use of the material is subject to the approval of (Name of Department). Application for obtaining permission should be made to (email address of the concerned Department).

Terms and conditions

Clearly worded terms and condition will set the rules and regulation that needs to be followed by the owner of the app and the users of the app.

Terms & Conditions shall address the following aspects:

1. Ownership Details
2. Usage Policy of Content
3. Legal Aspects

Sample Terms and Conditions

The App is designed, developed and maintained by (Name of the Department) Government of India.

Though all efforts have been made to ensure the accuracy and currency of the content on this app, the same should not be construed as a statement of law or used for any legal purposes. In case of any ambiguity or doubts, users are advised to verify/check with the Department(s) and/or other source(s), and to obtain appropriate professional advice.

Under no circumstances will this Department be liable for any expense, loss or damage including, without limitation, indirect or consequential loss or damage, or any expense, loss or damage whatsoever arising from use, or loss of use, of data, arising out of or in connection with the use of this app.

These terms and conditions shall be governed by and construed in accordance with the Indian Laws. Any dispute arising under these terms and conditions shall be subject to the jurisdiction of the courts of India

You must comply with App T&Cs as these apply to your use of the App and the Service T&Cs apply to your use of the Service that you access and use through the App. Any violation of these App T&Cs or the Service T&Cs may result in the termination of your access to the App and/or the Service.

The App is for your own personal use only. Any commercial use will result in termination of your access to the app and service. You cannot distribute or copy or modify any part of it in any way.

You must not attempt to extract any source code from the App, disassemble it or make any derivative versions, or attempt to interrupt or decipher the transmissions between the App and our systems.

The user of the app must not use the app for any the following:

1. Unlawful, malicious or criminal activity;
2. Defamatory, harassing or threatening activity. This includes any information that you may add or upload to the app;
3. Create disruption in service for other users of the app;

You must not use the App in a way that may damage or impair the App, the Service or the underlying systems and security.

The App and all copyright, database rights, and other intellectual property rights related to it belong to us.