

Avast Clean Guidelines

Advertising

MUST HAVE:

1. Landing page

- A landing page of a downloadable software must have a clear vendor identification, description of the software functionality, cost of the software (where applicable) and the fact that the software is ad supported. Further, such landing page must include an accessible EULA and Privacy Policy of the software.
- List of all bundled software, 3rd party components/dependencies (i.e. monetization engines), plugins or widgets.
- Link to product's EULA and Privacy Policy.
- All information must be presented in a way that meets industry standards for readability (i.e. no green font on a greenish background, no tiny letters...).

2. Disclosure and consent

- All app promoting pages must have clearly identified vendor.

PROHIBITED:

1. Misleading ads:

- All forms of threatening message.
- All forms of deceptive behavior (i.e. missing codecs, plugins, vulnerable/infected machine, when there is no need for such thing).
- All forms of impersonation of system messages (Windows UI, MSFT/Windows logo...), other brands (Chrome, Flash, anti-malware...) or web components (download buttons...).
- Displaying multiple "calls to action" with different wording leading to similar action.
- Advertising a free product for a cost.

2. Download

- Auto or direct download from ads is strictly prohibited.

3. Disclosure and consent

- Start app download/installation without proper disclosure and user consent.

Installation Process

RECOMMENDED:

1. Signing software

- Every executable file should contain a vendor identifier. No specific format is required, but Version Info is preferred. Other option could be a plaintext description in a custom section.
- Digital signature is always beneficial.
- If the file is packed, it should have a Taggant.

MUST HAVE:

1. Bundling software

- All programs offered to users should be legitimate in nature and should have a clear, positive value to the installing user.
- Each program must be offered in its own offer/install screen with clear information about functionality, behavior, cost (where relevant) and purpose of the software it offers.
- Each offer screen must have clearly labeled skip/decline button or opt-in/opt-out checkbox which enable the user to decline the offer.
- Each offer screen must have the same wording, “Call to Action” buttons, navigation style and button placement through the installation process.
- Any software that includes 3rd party components or software therein must provide appropriate disclosure to end users.

2. User consent, control and transparency

- All disclosure and consent clauses must be unavoidable to end users, must meet industry standards for readability a must be presented in a language that an ordinary end user comprehends.
- User consent must be obtained before download/installation of any software.
- Installer will install only software which user provided their consent to install.
- User must be able to stop the installation at any point.
- Any data acquisition shall be made under the end user’s consent.
- Each setup screen must include exit functionality.
- App installation must not be affected by any user decisions on the offers.
- App must disclose to user name of product, identify developer name or brand name as the providing entity, how to contact such entity.
- Software’s EULA must disclose to user if and how app may affect any other programs on user PC and settings.
- It must be clear in which stage the installation currently is and show progress during longer stages (i.e. while copying/downloading files).

3. Misleading behavior

- All app's functionalities must correlate with the description mentioned in the installation screens.

4. Update

- Software updater can only update main application (must not install any additional software without user consent).

PROHIBITED:

1. Bundling software

- Software without offer screens.
- Any form of promoting exaggerated or false claims about user system (health, registry, files, etc...).

2. User consent, control and transparency

- Sell or otherwise share user personal identifying information to 3rd parties without user explicit consent.
- Any software must have its own privacy policy to describe its data collection, usage and sharing practices.
- Software must not bypass/hack system or other apps security and consent features (browser hijack, disable notification...).
- Software must not operate, access any content or cause use of user's pc without prior informed consent (i.e. operate BitCoin miners).
- Software must not redirect/block/modify searches, queries, user-entered URLs etc. without user consent.
- Software must not access any other site that doesn't directly relate to consented software functionality.
- Any type of installation which does not require the End Users' informed consent is expressly prohibited.

3. Misleading behavior

- Installer must not mislead a user to take action he has previously declined.
- Revenue modules must not engage with fictional installations of the product or the revenue model.
- All forms of displaying exaggerated/misleading/inaccurate claims about the system's health/files/registry or other items on the system are strictly prohibited.
- Installer must not initiate install of app based on false/misleading/fraud representation.
- Software must not falsely claim to be a program from other brands (Avast, Microsoft, Google, Adobe...).

4. Interfering

- Software must not engage with interfering, replacing, uninstalling or disabling any third party content, application, browser functionality and/or settings, websites, widget, the operating system or any part thereof without user consent.
- Software must not engage in any fraud activity.
- Software must not interfere with browser default search/search pages without the user's consent.

Program functionality:

MUST HAVE:

1. Transparency and attribution

- Ads must include clear attribution to the providing application.
- Ads must be clearly labeled and identified as such.
- When injecting data into external content (such as website, search results..), monetization services must be clearly labeled and identified as distinguished from any content (such as website) it appears on.
- Ad will carry a link to an "Ad Info" webpage with the following prominent notices and information: a short explanation about why the Ads was displayed, links to the Advertiser's full and clear description of the revenue module, links to the Product's terms of service and privacy policy.

PROHIBITED:

1. Transparency and attribution

- A program must not fail to clearly indicate when the program is active, and must not attempt to hide or disguise its presence.

2. Program behavior

- Software must not include monetization services that are Pop-Ups, Pop-Unders, Expanding banners etc.
- Software will not use the end user's device for purposes that are unwarranted and unexpected by the end user.
- Software may not decrease computer reliability and/or cause a poor end user experience.
- Uninstall.

MUST HAVE:

- Once a user uninstalled an app and/or monetization module attributed to that specific app, it must completely remove all components with no remains on the user's PC.
- The uninstall process should function properly and be a mirror of the installation process
- The installed software must have a corresponding "Add/Remove" entry in Windows Control Panel or equivalent on different platforms, and the user must be able to completely uninstall.
- Software name (as was shown in the installation process and operation of the app and/or monetization module) must be identical to the one in the OS add/remove in control panel.
- Software or the ads attributed to it must have an easy way to close them.

Privacy Policy and EULA

MUST HAVE:

1. Privacy Policy

- App and/or monetization service's privacy policy shall comply with applicable privacy and data collection and protection laws, and shall provide a clear and comprehensive description of the Advertiser's data collection practices.
- Privacy Policy must describe:
 - If software uses cookies or other means of collecting User data.
 - If software access/collect/use/disclose user's PII.
 - What user data is accessed/collected/used/disclosed and how, what means it uses to do so and what is done with the data collected.
 - How a user can notify that they wish to opt out from PII collection and have the app and/or monetization service stop collecting PII data about them. Users must be able to achieve this in a straightforward way, and app and/or monetization service must comply with the users' wish immediately.

2. EULA

- App and/or monetization service must comply with applicable law, must have EULA that is accessible during the installation process and from the app's website, vendor and product must comply with EULA (as consented by user, and was available in install and on product).
- App and/or monetization service should be described in a clear EULA, any material change to the EULA must have user consent.

PROHIBITED:

1. Privacy Policy

- App and/or monetization service must not sell or otherwise share with third parties personally identifying information without the end user's prior specific consent.
- App and/or monetization service must not mislead users about the origin of cookies and/or other means of collection of data, or cause user to believe it's associated with another app.