+++ title = “Plugin publishing and signing criteria” +++

Plugin publishing and signing criteria

Grafana plugins must adhere to the following criteria when being reviewed for publishing and signing.

Privacy and security

- Plugins cannot collect usage or user information. Violations of this include but is not limited to:
  - Directly collecting installation and user statistics
  - Sending data to 3rd parties for analytics purposes
  - Embedding tracking code
- Data at rest: sensitive data such as credentials and user information, must be encrypted using industry standards.
  - Use secureJsonData to store data source credentials
  - Secrets cannot be stored in panel options
- Data transmission: secure methods that meet industry standard encryption levels should be used, such as Secure Sockets Layer (SSL) or Transport Layer Security (TLS)
- Abuse: plugins should not perform actions beyond the scope of the intended use.
  - Do not include hidden files
  - Do not manipulate the underlying environment, privileges, or related processes

Commercial

- Usage of 3rd party software or dependencies within the plugin must be licensed for the intended use. For example, using open source dependencies must be credited/licensed; embedding logos or trademarks;

Grafana Labs reserves the right to decline or remove any plugin at its discretion. Failure to comply with publishing and signing criteria may result in immediate removal from the Grafana plugin catalog.