Powered by Firefox OS Branding Requirements

This document contains obligations you must meet in order to use the Powered by Firefox OS Brand Assets in conjunction with the distribution of Branded Devices. The names "Mozilla", "Firefox" and "Firefox OS" identifies Mozilla's brand and represents Mozilla's values and ideals. This document may be updated from time to time by Mozilla to reflect current requirements.

	Powered by: Firefox OS
Brand Assets available	Brand assets available: "Powered by Firefox OS" tier as described in the Brand Kit.
Your use cases	Branded Devices that meet minimum compatibility requirements
Requirements	Branded Devices must pass the following requirements: * Open Source License Compliance * Pass the Open Web Device Compliance Review Board * Meet Performance and Compatibility Requirements
Firefox Marketplace and Mozilla services	Firefox Marketplace and other Mozilla Services available.

1. **Definitions**.
   a. "**APIs**" are application programming interfaces that allow other programs, such as web apps, to interact with a given program.
   b. "**Open Web Device Compliance Review Board**" or "**OWDCRB**" means a third party entity created by Mozilla and other third parties to encourage API compatibility and performance baselines for Branded Devices.
   c. "**Mozilla Contact**" means the Mozilla contact identified in your Mozilla Brand Certification Letter, or such other contact Mozilla may designate from time to time.
   d. "**Web APIs**" are APIs in the operating system that are exposed for access by a web application and does not include private internal facing APIs not exposed for access by a web application.
2. **Branding Tiers**.
   a. "**Powered by Firefox OS**"
      i. You may create Branded Devices bearing the "Powered By Firefox OS" tier of branding described in the Brand Kit.
      ii. Should you wish to use the "Powered by Firefox OS" brand tier, you must adhere to the following requirements:

A. Open Source License Compliance (requirements below)

B. Performance and Web Compatibility Requirements (see below)

iii. You must follow the Review and Approval Processes for "Powered by Firefox OS" described in Section 5 of this Exhibit A.

iv. Once you have met the requirements above, you may use the applicable branding for the "Powered by Firefox OS" tier in the manner described in the Brand Kit. **NOTE**: You may ONLY use the assets detailed under "Powered by Firefox OS" tier in the Firefox OS Brand Identity Guidelines for Branded Devices meeting this tier of branding and not any other Mozilla Marks or brand assets.

3. Open Source License Compliance. Your distribution of any open source object or source code must comply with the requirements for each of the open source licenses governing that code. There is more information about the open source in Boot2Gecko available at https://wiki.mozilla.org/Boot2Gecko/Licensing. Mozilla strongly recommends you getting involved in and consider making open source contributions back to the Boot 2 Gecko project. To find out more about how to get involved, please see the following resources:

a. https://developer.mozilla.org/en-US/docs/Introduction

b. https://developer.mozilla.org/en-US/docs/Mozilla/Firefox_OS

c. http://mozilla.github.io/process-releases/draft/development_overview

d. https://wiki.mozilla.org/B2G/Architecture

e. https://wiki.mozilla.org/WebAPI

4. Platform Compatibility and Performance. Should you wish to create Branded Devices, they must adhere to the following requirements:

a. *Open Web Device Compliance Review Board*. Mozilla, along with operators, chipset manufacturers and other third parties have created the Open Web Device Compliance Review Board to encourage web API compatibility and performance baselines for devices. The OWDCRB is slated to fully launch in Q3 of 2014. Once the OWDCRB is launched, in order to create Branded Devices using either tier, each Device must first pass the OWDCRB. There are limited exceptions to this requirement that Mozilla may grant in its sole discretion (such as if there are no performance metrics for the type of device you are creating) and you should contact the Mozilla Contact if you believe a Branded Device may qualify for such an exception. You can learn more and start the OWDCRB process by visiting https://www.openwebdevice.org.

b. *Minimum Hardware Requirements*. All Branded Devices must meet the following minimum hardware and software requirements:

i. **Mobile phones** (for "Firefox OS 1.x"):

1. CPU: Minimum 1GHz, single-core, equivalent to ARM Cortex A5 processor
2. Storage: 256MB
3. System RAM: 128MB
4. Display: 262k color, 3.5-inch HVGA (480x320) capacitive multi-touch display (minimum two points)

5. GPU: WebGL-capable GPU capable of rendering H.264 video at 30FPS
6. Hardware Buttons: Home, Power, Volume up, Volume down. Back, Menu, and Search hardware buttons may NOT be present on a Firefox OS Co-branded.

ii. **Other devices**: Requirements for other devices are to be approved by Mozilla in writing.

c. *Web API Compatibility*

i. Requirement: Because cross compatibility of Firefox OS is critical to the success of the platform, without obtaining prior written approval from Mozilla, you shall not add, remove or modify any default functionality regarding the compatibility of web sites and web applications in Branded Devices. Mozilla welcomes innovation across the open source Firefox OS platform. If you see a need to add, remove or modify Web APIs, you will reach out to your Mozilla Contact to discuss alternatives or work with Mozilla to standardize such changes in a mutually acceptable way.

ii. Clarifications: The following are further clarifications regarding the foregoing requirement:

1. Unless approved in writing by Mozilla (including via email), you shall not add, remove or modify any APIs found in files in Branded Devices which are exposed to web content, including certified, privileged or regular apps and general web pages. For example:
    i. You shall not modify APIs declared in files with "idl" or "webidl" extensions.
    ii. You shall not add, remove, or modify HTML elements and their attributes, other Web languages such as SVG and MathML, CSS properties, application manifests, permissions, and any other similar functionality available to web pages and applications.
2. You shall not modify the default user agent string and shall ensure the Gecko user agent string is accurate to the appropriate version of Gecko. More information may be found here:
    i. https://wiki.mozilla.org/B2G/User_Agent/OEM_Changes_Policy
    ii. https://developer.mozilla.org/en-US/docs/Gecko_user_agent_string_reference
3. You shall not modify the behavior of existing Web APIs. For example, you shall not change the semantics of a function or its side effects.
4. You shall not remove any functionality found in existing Web APIs (such as removing media formats, HTML elements, DOM properties or methods, etc.) or any Web APIs themselves.

d. *Ongoing Compatibility Through Updates*. You shall ensure that Branded Devices are provided with the following update requirements for a period of at least **1 year** (or longer if required by applicable law) from the first commercial launch date of each applicable such Branded Device:

Mozilla will release source code for upgrades and updates, including any security fixes, according to the release schedule and process it generally uses for software development. For each such update or upgrade, you will comply with the update

testing, certification and deployment schedule set forth in Appendix 1 below. All updates will be made available by Mozilla in source code form and you will complete all builds into executable form. For any update deployed by you, you will give end users notice and choice over whether to accept such update, including without limitation by the end user enabling default updating. This requirement shall survive any termination or expiration of the Agreement.

e. *Compatibility Through not Modifying Permission Architecture or Data Management Features*. You will not make modifications to Branded Devices in such a way that any security or data management feature (or their respective default configurations) are changed, including:

   i. Branded Devices must implement the permission model and trust levels documented here:

      1. https://developer.mozilla.org/en-US/docs/Mozilla/Firefox_OS/Security/Security_model
      2. https://developer.mozilla.org/en-US/docs/Mozilla/Firefox_OS/Security/System_security

   ii. Branded Devices must gate access to Web APIs by appropriate permission checks. Current permissions checks are documented here:

      1. https://developer.mozilla.org/en-US/docs/Web/Apps/App_permissions

   iii. Applications that are pre-installed on a Branded Device that are derived from the Firefox Marketplace should ship with the app signing certificate provided for Firefox Marketplace and pre-installed applications that do not derive from the Firefox Marketplace must not use the Firefox Marketplace signing certificate.

   iv. You must not modify the operation of the following features in Branded Devices:

      1. Do Not Track flag
      2. The user-controlled clearing of application data (including, without limitation, for any pre-installed applications)
      3. The default operation of any Mozilla Services integrated into the Branded Devices (such as update data pings and crash reporting).

   v. You will not introduce any spyware or malware into Branded Devices. Additionally, you will not use other means, without an end user's consent, for you or any third parties to access a user's personal information.

   vi. You will not make any modifications to Branded Devices that would cause the Firefox OS privacy policy (available at http://www.mozilla.org/en-US/privacy/policies/firefox-os/) or the Firefox Marketplace Privacy Policy (available at https://marketplace.firefox.com/privacy-policy), in each case as modified from time to time, to no longer be accurate.

5. Review Process; Audit.

i. *Of Devices/Builds*.

   1. When available, you shall complete the OWDCRB certification process (available at https://www.openwebdevice.org).

2. You shall complete the Powered by Firefox OS Self Certification Checklist (to be made available here at: http://www.mozilla.org/firefoxos/certification) and shall submit such checklist along with a sample of the Branded Device being together with mocks of final packaging to the address specified by Mozilla.

ii. *Of Marketing*. Mozilla provides the Brand Kit for Branded Devices by the "Powered by Firefox OS" level of branding ("**Firefox OS Brand Toolkit**"). You may only use such assets provided under the Firefox OS Brand Toolkit in the manner described therein **with no modifications**. For clarity, nothing in the Firefox OS Co-branded Brand Toolkit described below may be used. Questions regarding the Firefox OS Brand Toolkit may be directed to the Mozilla Contact.

iii. *Audit*. Mozilla shall have the right to audit your compliance with this Exhibit A. Mozilla shall advise you of any non-conformity with these Firefox OS Brand Requirements, and you will promptly update Branded Devices to resolve such non-conformity. Mozilla has the right to take all action that it deems necessary to ensure that your activities under and uses of the Mozilla Marks are consistent with the reputation for quality and prestige of products bearing the Mozilla Marks, including any quality standards.

Appendix 1: Updates Schedule

Type	Release Frequency (Mozilla)	Your Push Commitment
Urgent Maintenance Update (Urgent, isolated security or product fix)	On an as-needed basis	As soon as possible, estimated to be no more than 2 weeks after code change made available that you need to have tested, certified and deployed to users
Security Update (important security fixes)	Releases made available every 6 weeks	At least once every 90 days, with regular 90 day cadence
OS Update (New features, bug fixes, security fixes)	Releases made available approximately once every 6 months	Deployed to users <180 days from when the update becomes available

- Mozilla will maintain Firefox OS repositories with major/critical security and usability fixes, along with any partner-required features.
- Mozilla will make source code available to you.
- You will perform all builds and updates and engage in appropriate testing and certification for such builds.
- Mozilla will provide Security Update patches available for the previous two OS Updates to you.
- You agree to test/certify the full set of security bug fixes for each Security Update that is deployed.
- Mozilla will converge a Firefox OS version 1.X build every 6 weeks, and bump the version number at that time.
- Mozilla will notify you as soon as Mozilla is aware of an Urgent Maintenance update, and will inform you so that they can follow along with the investigation/fix.
- You acknowledge that if there is an update available at phone launch, they will pick up security/stability/usability/partner-feature change accumulated during the device launch gap and agree to generate and deploy such update within 2 weeks of launch.
- Urgent Maintenance updates will be indicated by incrementing the 3rd digit of the version number of the most recent release branch. When you take only that change on top of your last released version should increment the 4th digit of your version number.