

Guidance for the Reuse of Mobile Devices

Guidance is intended to offer further explanation of complex requirements in the R2 Standard along with examples and audit recommendations. However, this document itself is not auditable and cannot be cited in relation to any nonconformances. The explanations within are intended to prevent misinterpretation of the R2 Standard, not to add to, subtract from, or modify the R2 Standard. The examples cited may not be the only way to fulfill a requirement of the standard.

Although reasonable care was taken in the preparation of this document, SERI and any other party involved in the creation of the document HEREBY STATE that the document is provided without warranty, either expressed or implied, of accuracy or fitness for purpose, AND HEREBY DISCLAIM any liability, direct or indirect, for damages or loss relating to the use of this document.

The information in this guidance focuses specifically on the application of the R2 Standard requirements in the refurbishment and reuse of mobile devices. While this guidance is written specifically with mobile devices in mind, the concepts may be applicable across other types of devices. This guidance is written in a question and answer format.

	Question	Answer
1.	What is the “blacklist”?	<p>The blacklist is a list of IMEIs (International Mobile Equipment Identity) that are associated with mobile devices that should be denied service on mobile networks because they have been reported as lost, stolen, faulty or otherwise unsuitable for use. This list is stored in the Central Equipment Identity Register (CEIR) which acts as a central system for network operators to share their individual black lists so that devices denied service (blacklisted) by one network will not work on other networks.</p> <p>https://www.gsma.com/aboutus/leadership/committees-and-groups/working-groups/fraud-security-group/fraud-imei-database</p> <p>https://www.gsma.com/managedservices/device-blacklist-services/recycling/</p>
2.	Can a blacklisted device be reused?	<p>No. It is illegal. The R2 recycler in possession of a lost or stolen device would not have the legal right to resell the device for reuse. A faulty device is not working, and determined to not be capable to be reused. Therefore a blacklisted device cannot be sold for reuse. It must first be removed from the blacklist for an R2 recycler to resell it.</p>
3.	Do connections to remote services need to be removed from a device in order to reuse it?	<p>Trends in technology are perpetually connecting devices to remote services in the cloud. Previous user connections to these remote services may not be effectively disabled by the sanitization process, enabling reconnection to the prior user’s account and/or the repopulation of the previous user’s data and information. This increases the risk of ineffective data sanitization when a device is transferred to another user for reuse.</p> <p>Provision 8.e requires quality controls “to ensure effectiveness of data sanitization, purging, and destruction techniques.” Quality controls should include verification that all logins, passwords, locks, or any other connections to a remote service are removed and no longer connected to the device. The device should leave no residual connection</p>

	Question	Answer
		to any prior user or service that is not included with the original device offering. Any connections that cannot be removed are residual data that require physical destruction to sanitize the device. These devices with the prior user’s connections are not reusable.
4.	What is a FMIP lock?	<p>FMIP stands for “Find My iPhone” lock. When this feature is activated, the Activation Lock is automatically turned on. The device is connected to a user account on the Apple Activation Servers. This prevents others from using the device even if they restore it to the original factory settings.</p>
5.	Do I need to check for an activation lock in the refurbishment process?	Yes. An activation lock (Apple, Android, etc.) may prevent the device from being properly sanitized of the prior user’s data and may impact the ability of the next user to use the device. Connectivity is required to adequately test the device. Therefore, the refurbishment process may require a SIM card to test the connections and verify activation locks have been removed.
6.	Can a device with an activation lock be reused under R2?	Devices with an activation lock are not reusable until the lock is removed. For this reason, these devices <u>cannot</u> be identified and sold as R2/Ready for Reuse nor R2/Ready for Resale in accordance with Provision 6.
7.	Can the parts of an activation locked phone be reused?	Yes, except for the circuit board and any other components (like the touch ID sensor) which would be impacted by the activation lock.

	Question	Answer
8.	Can an activation lock be removed?	<p>SERI is not currently aware of any legal ways to remove the iCloud activation lock without the intervention of the user who activated the lock or by Apple. Other methods described on the Internet appear to be temporary workarounds or nefarious actions that are likely illegal. SERI presumes that the following actions, at a minimum, are not legal:</p> <ol style="list-style-type: none"> 1. Changing the serial number on the device; or 2. Changing the IMEI number on the device; or 3. Replacing the chips holding the IMEI or serial number of the device.
9.	Is a device with an iCloud activation lock erased of the user's data?	<p>It is possible that the data from the previous user could be repopulated even if iOS recovery mode is used to restore the device to factory defaults. Therefore, SERI presumes a device with an iCloud activation lock to not be sanitized and would require additional data sanitization, including legal removal of the activation lock.</p>
10.	Can a device with an activation lock or other residual connection be imported to Hong Kong?	<p>Hong Kong Environmental Protection Department (EPD) has published advice on the import of used electronic equipment. Electronic devices with a battery which are not ready to “be reused for their originally intended purpose without repair” are likely hazardous wastes under Hong Kong laws. Furthermore, Hong Kong will not issue a permit to import hazardous wastes from a developed country, such as the United States. Therefore, SERI presumes it to be illegal to import most mobile devices that have any type of residual lock or connection, unless it can be clearly demonstrated by the R2 organization with evidence from the Hong Kong EPD to be legal.</p> <p>However, those devices with the battery removed and not included in the shipment would probably be uncontaminated electronic scrap (GC020) and therefore likely legal to import from any country without an import permit. Under R2 Provision 3.a.2, it is the R2 recycler's responsibility to demonstrate the legality of each shipment to be imported prior to shipment, including those made by the R2 recycler's downstream vendors.</p> <p>http://www.epd.gov.hk/epd/sites/default/files/epd/english/environmentinhk/waste/guide_ref/files/advice_on_e-waste.pdf</p>