Open #iotmark principles

March 9th 2018

	Privacy	Interoperability	Openness	Data governance	Permissons	Transparency	Security	Lifecycle
Must have	The connected product supplied by the organisation is GDPR compliant. The organisation doesn't sell customer data without consent. Customer data isn't used for profiling, marketing or advertising without transparent disclosure.				The organisation gives users the ability to transfer ownership of the device. When ownership of a device is transferred, the new user doesn't have access to the previous user's data.	The organisation makes it explicit to the user what the implications of substantially changing usage of the device are. The organisation makes explicit the expected duration of the terms of service. The organisation asks the explicit permission of the customer when it wants to change the length of the terms of service. The organisation informs the user about firmware upgrades.	The organisation enforces a strong user identity policy. The organisation has clear admin user management policies. The organisation provides minimum cryptographic security on its backend & secure configuration. The device firmware is compliant with industry security standards.	The organisation lets a user do a factory reset on the device. The organisation is clear about the expected lifetime of the service provided by the device and backend. The organisation is clear about the levels of customer support that are provided during the lifetime of the product.
Nice to have		The organisation grants third parties the same functional scope on the backend as its own clients. The organisation allows third parties to communicate directly with its devices without going through the backend. The organisation allows third parties to connect clients to its backend.		The organisation doesn't degrade or change the current core functionality of the device over the product lifetime. The organisation makes it possible for customers to turn off the connection to the backend, this might mean that functionality of the device is reduced.	The organisation lets users export their data.		The organisation implements reliable and appropriate backend patching procedures which are evidenced. The device uses strong cryptographic schemes.	The organisation supplies a list of the first level of suppliers involved in their supply chain. The organisation supplies spare parts on request during the lifecycle of the product. The organisation supplies a list of the geographic regions involved in the supply chain. The organisation gives clear documentation for any parts that a customer can repair using commonly accessible tools and skills.
Best scenario		The organisation allows third parties to connect devices to its backend.	The organisation publishes the device source code under an open source license. The organisation publishes the device hardware designs under an open hardware license. The organisation publishes the backend source code under an open source license.				The organisation's backend implements additional secure setup options.	

This poster is a workshop tool to test industry interest in the principles of an open internet of things certification mark.

See iotmark.org for more details.