Online Trust Alliance

OTA IoT Trust Framework – Released 3/2/2016

The IoT Trustworthy Working Group (ITWG) first established in January 2015, is a multi-stakeholder initiative chartered with developing a **IoT Trust Framework** addressing security, privacy and sustainability in IoT products and services. The initial scope of this effort focuses on the connected / smart home and connected home products and 2) consumer facing wearable technologies. The IoT Trust Framework and emphasizes that "security and privacy by design" must be a priority from the onset of product development and be addressed holistically. To assist in the implementation and adoption of the framework, OTA has a companion **IoT Trust Framework Resource Guide** with expanded explanations, examples, best practices and resources. Both this Framework and the Resource guide are available at https://otalliance.org/IoT. Updates and revisions will also be posted to that location. Additional consumer resources may be found at https://otalliance.org/SmartHome.

Note adherence to the Framework does not override regulatory requirements nor does it mean compliance with the law and/or regulations. The framework represents rough consensus of the ITWG.

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	**Connected Home**	**Wearable Tech**
SECURITY		
1. Ensure devices support current generally accepted security transmission protocols. All personally identifiable data in transit and in storage must be encrypted using current generally accepted security standards. This is including but not limited to wired, WI-FI and Bluetooth connections.	●	●
2. All authentication credentials, including but not limited to passwords shall be salted and hashed and/or encrypted.	●	●
3. All IoT support web sites must fully encrypt the user session. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL.	●	●
4. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform generally accepted penetration tests at least annually.	●	●
5. Establish and maintain processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including the research community. Remediate post product release design vulnerabilities and threats in a publically responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s).	●	●

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	Connected Home	Wearable Tech
6. All software and/or firmware updates, patches and revisions must either be signed and/or otherwise verified as coming from a trusted source. Updates and patches should not modify user-configured preferences, security and/or privacy settings without user notification.	●	●
7. Ensure all IoT devices and associated software, have been subjected to a rigorous, standardized software development lifecycle process including unit, system, acceptance, regression testing and threat modeling, along with maintaining an inventory of the source for any third party/open source code and/or components utilized. Employ generally accepted code and system hardening techniques.	●	●
8. End-user communications including but not limited to email and SMS, must adopt authentication protocols to help prevent spear phishing and spoofing. For example for email communications must adopt SPF, DKIM and DMARC, for all security and privacy related communications and notices.	●	●
9. For email communications within 180 days of publishing a DMARC policy, implement a reject policy, helping ISPs and receiving networks to reject email which fail email authentication verification checks.	○	○
10. IoT vendors using email communication must adopt transport-level confidentiality including generally accepted security techniques for email to aid in securing communications and enhancing the privacy and integrity of the message.	○	○
USER ACCESS & CREDENTIALS		
11. For user access, provide unique system generated or single use passwords; or alternatively use secure certificate credentials. As necessary, require use of unique passwords for administrative access, delineating between devices and services and the respective impact of factory resets.	●	●
12. Provide generally accepted recovery mechanisms for IoT application and support passwords and/or mechanisms for credential re-set using multi-factor verification (email and phone, etc.) where no user password exists.	●	●
13. Companies must take steps to protect against 'brute force' and/or other abusive login attempts (such as automated login bots, etc.) by locking or disabling user and device support account(s) after a reasonable number of invalid log in attempts.	●	●
14. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).	●	●
15. Enact a breach response and consumer notification plan to be reevaluated, tested and updated at least annually or after significant internal system, technical and / or operational changes.	●	●

PRIVACY, DISCLOSURES & TRANSPARENCY		
IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	**Connected Home**	**Wearable Tech**
16. Ensure privacy, security and support policies are easily discoverable, clear and readily available for review prior to purchase, activation, download or enrollment. In addition to prominent placement on their website, it is recommended companies utilize QR Codes, user friendly short URLs and other similar methods.	●	●
17. Disclose the duration of security and patch support, (beyond product warranty). Such disclosures should be aligned the expected lifespan of the device.	●	●
18. Conspicuously disclose what personally identifiable and sensitive data types and attributes are collected and how they are used, limiting collection to data which is reasonably useful for the functionality and purpose for which it is being collected. Disclose and provide consumer opt-in for any other purposes.	●	●
19. Disclose what features will fail to function if connectivity becomes disabled or stopped including but not limited to the potential impact to physical security.	●	●
20. Disclose the data retention policy and duration of personally identifiable information.	●	●
21. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding and/or connecting with other devices, platforms or services.	●	●
22. Publically disclose if and how IoT device/product/service ownership may be transferred (e.g., a connected home being sold to a new owner or sale of a fitness tracker).	●	●
23. Only share consumers' personal data with third parties with consumers' affirmative consent, unless required and limited for the use of product features or service operation. Require third party service providers are held to the same polices including holding such data in confidence and notification requirements of any data loss/breach incident and/or unauthorized access	●	●
24. Provide controls and/or documentation enabling the consumer to review and edit privacy preferences of the IoT device including the ability to reset to the "factory default."	●	●
25. Commit to not sell or transfer any identifiable consumer data unless it is a dependent part of the sale or liquidation of the core business which originally collected the data, providing the acquiring party's privacy policy does not materially change the terms. Otherwise notice and consent must be obtained.	●	●
26. Provide the ability for a consumer to return a product without charge after reviewing the privacy practices that are presented prior to operation, provided that such terms are not conspicuously disclosed prior to purchase. The term (number of days) for product returns shall be consistent with current exchange policies of the retailer, or specified in advance.	●	●

IoT Trust Framework ● Required ○ Recommended N/A – Not Applicable	Connected Home	Wearable Tech
27. Whenever the opportunity is presented to decline or opt out of any policy, the consequences must be clearly and objectively explained, including any impact to product features or functionality. It is recommended the end-user value of opting in and/or sharing data be communicated to the end-user.	●	●
28. Publically post the history of material privacy notice changes for a minimum of two years.	○	○
29. Provide the ability for the user or proxy to delete, or make anonymous personal or sensitive data stored on company servers (other than purchase transaction history) upon discontinuing, loss or sale of device.	○	○
30. Provide device or service data erasure and zeroization in the event of loss or sale.	○	○

Terminology, Definitions & Clarifications

1. Unless specified otherwise, the terms device manufacturers, vendors, application developers, service providers and platform operators are all indicated by the term "Companies." The inclusion of platforms is paramount as the IoT may be headed to a future where platform and OS providers and their respective connected ecosystems communicating on a seamless network may pose security and privacy risks.
2. It is expected that companies, products and services are in compliance with any law or regulation of the jurisdiction that governs the collection and handling of personal and sensitive information. Failure to do so constitutes non-compliance with this framework and results in automatic disqualification from any forthcoming code of conduct or certification program.
3. It is expected companies disclose details of sharing data with law enforcement and reference any applicable transparency reports as legally permitted.
4. Smart devices refer to devices (and sensors) which are networked and may only have one-way communications.
5. Medical devices regulated by the FDA are beyond the scope of the Framework, yet the majority of the criteria are deemed to be applicable.