

IoT Trust Framework ● Required ○ Recommended	
Security – Device, Apps and Cloud Services	
1. Ensure devices and associated applications support current generally accepted security and cryptography protocols and best practices. 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 IoT support web sites must fully encrypt the user session, from the device to the backend services. Current best practices include HTTPS or HTTP Strict Transport Security (HSTS) by default, also known as AOSSL or Always On SSL. Devices should include mechanisms to reliably authenticate their backend services and supporting applications.	●
3. IoT support sites must implement regular monitoring and continual improvement of site security and server configurations to acceptably reduce the impact of vulnerabilities. Perform penetration tests at least annually.	●
4. Establish coordinated vulnerability disclosure including processes and systems to receive, track and promptly respond to external vulnerabilities reports from third parties including but not limited to customers, consumers, academia and the research community. Remediate post product release design vulnerabilities and threats in a publicly responsible manner either through remote updates and/or through actionable consumer notifications, or other effective mechanism(s). Developers should consider “bug bounty” programs, and crowdsourcing methods to help identify vulnerabilities that companies’ own internal security teams may not catch or identify.	●
5. Must have a mechanism for automated safe and secure methods to provide software and/or firmware updates, patches and revisions. Such updates 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. Automated (vs automatic) updates provide users the ability to approve, authorize or reject updates	●
6. Ensure all IoT devices and associated software, have been subjected to a rigorous, standardized software development lifecycle process and methodologies 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 across a range of typical use case scenarios and configurations, including preventing any data leaks between the device, apps and cloud services. Developing secure software requires thinking about security from a project’s inception through implementation, testing, and deployment. Devices should ship with reasonably current software and/or on first boot push automatic updates to address any known critical vulnerabilities.	●
7. Conduct security, and compliance risk assessments for all service and cloud providers. (See resource guide for recommendations).	●
8. Develop and maintain a “bill of materials” including software, firmware, hardware and third party software libraries (including open source modules and plug ins). (This would apply to the device, mobile and cloud services to help quickly remediate disclosed vendor or open source vulnerabilities)	○
9. Design devices to minimum requirements necessary required for operation. For example, USB ports or memory card slots should only be included if they are required for the operation and maintenance of the device. Unused ports and services should be disabled.	●
User Access & Credentials	
10. Include strong authentication by default, including providing 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.	●

IoT Trust Framework ● Required ○ Recommended	
11. Provide generally accepted recovery mechanisms for IoT application(s) and support passwords and/or mechanisms for credential re-set using multi-factor verification and authentication (email and phone, etc.) where no user password exists.	●
12. 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.	●
13. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).	●
14. Authentication credentials including but not limited to user passwords shall be salted, hashed and/or encrypted. Applies to all credentials stored to help prevent unauthorized access and brute force attacks.	●
Privacy, Disclosures & Transparency	
15. 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 product packaging, on their website, it is recommended companies utilize QR Codes, create user friendly short URLs and other similar methods maximizing disclosure at point-of-purchase.	●
16. Disclose the duration and end-of-life security and patch support, (beyond product warranty). Such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase. <i>(It is recognized IoT devices cannot be indefinitely patched. Consider communicating the risks of using a device beyond its usability date, and impact and risk if warnings are ignored or the device is not retired).</i>	●
17. 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.	●
18. Disclose what and how features will fail to function if connectivity or backend services becomes disabled or stopped including but not limited to the potential impact to physical security. <i>(Consider building in controls to disable connectivity or disable ports to mitigate potential threats, while maintaining core product functionality, based on the device usage, balancing out potential life/safety issues).</i>	●
19. Disclose the data retention policy and duration of personally identifiable information stored.	●
20. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.	●
21. Publicly disclose if and how IoT device/product/service ownership and the data may be transferred (e.g., a connected home being sold to a new owner or sale of a fitness tracker).	●
22. 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 that 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.	●
23. 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.”	●
24. 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.	●
25. 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	
26. 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.	●
27. Comply with applicable regulations including but not limited to the Children’s Online Privacy Protection Act (COPPA) and international privacy, security and data transfer regulatory requirements.	●
28. Publicly post the history of material privacy notice changes for a minimum of two years. Best practices include date stamping, redlines, and summary of the impacts of the changes.	●
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 the ability to reset a device and application to factory settings, providing the ability for erasure and zeroization in the event of transfer, loss or sale.	○
Notifications & Related Best Practices	
31. End-user communications including but not limited to email and SMS, must adopt authentication protocols to help prevent spear phishing and spoofing. Domains should implement SPF, DKIM and DMARC, for all security and privacy related communications and notices as well as for parked domains and those that never send email.	●
32. For email communications within 180 days of publishing a DMARC policy, implement a reject or quarantine policy, directing ISPs and receiving networks to reject email which fails authentication verification checks.	○
33. IoT vendors using email communication must adopt transport-level confidentiality including generally accepted security techniques to aid in securing communications and enhancing the privacy and integrity of the message.	○
34. Implement measures to help prevent or make evident any physical tampering of devices. Such measures help to protect the device from being opened or modified for malicious purposes after installation or from being returned to a retailer compromised.	○
35. Consider how to accommodate accessibility requirements for users who may be vision, hearing and or mobility impaired to maximize access for users of all physical capabilities.	○
36. Develop communications processes to maximize user awareness of any potential security or privacy issues, end-of life notifications and possible product recalls, including in app notifications. Communications should be written maximizing comprehension for the general user’s reading level. Consider multi-lingual communications recognizing that English may be the “second language” for users (see related principles regarding security and message integrity).	●
37. Enact a breach and cyber response and consumer notification plan to be reevaluated, tested and updated at least annually and/or after significant internal system, technical and / or operational changes.	●
<p>For Updates and resources including the IoT implementation guide visit https://otalliance.org/IoT</p>	
<p>© 2017 Online Trust Alliance. All rights reserved. Material in this publication is for educational and informational purposes only. Neither the Online Trust Alliance (OTA), its members, nor the authors assume any liability for any errors or omissions nor how this publication or its contents are used or interpreted or for any consequences resulting directly or indirectly from the use of this publication. For legal advice or any other, please consult your personal attorney or appropriate professional. The views expressed in this publication do not necessarily reflect the views of OTA member companies or affiliated organizations. OTA MAKES NO WARRANTIES, EXPRESS, IMPLIED, OR STATUTORY, AS TO THE INFORMATION IN THIS DOCUMENT. No part of this publication may be reproduced or distributed in any form or by any means, or stored in a database, web site or retrieval without the written consent and license by OTA.</p>	

r1/5/17