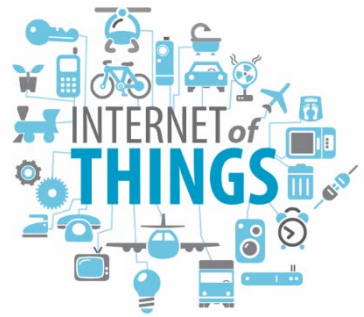
Online Trust Alliance
an Internet Society Initiative

IoT Security & Privacy Trust Framework v2.5

The IoT Trust Framework® includes a set of strategic principles necessary to help secure IOT devices and their data when shipped and throughout their entire life-cycle. Through a consensus driven multi-stakeholder process, criteria have been identified for connected home, office and wearable technologies including toys, activity trackers and fitness devices. The Framework outlines the need for comprehensive disclosures which to be provided prior to product purchase articulating policies regarding data collection, usage and sharing, as well as the terms and conditions of security patching post warranty. Security updates are essential to maximize the protection of IoT devices when vulnerabilities are discovered and attacks evolve. In addition, the Framework provides recommendations for manufactures to enhance transparency and communication of the devices' ability to be updated as well as data privacy related issues.



Core to addressing the inherent security risks and privacy issues is the application of the principles to the entire device solution or ecosystem. These include the device or sensor, the supporting applications, and the backend / cloud services. As many of the products coming to market rely on third party or open source components and software, it is incumbent on developers to apply these principles and conduct supply chain security and privacy risk assessments.

Serving as a risk assessment guide for developers, purchasers and retailers, the Framework is the foundation for future IoT certification programs. It is the goal of OTA to highlight devices which meet these standards to help consumers, as well as the public and private sectors, make informed purchasing decisions. The Framework and related resources are available at https://otalliance.org/IoT.

The Framework is broken down into 4 key areas:

- **Security Principles** (1-12) – Applicable to any device or sensor and all applications and back end cloud services. These range from the application of a rigorous software development security process to adhering to data security principles for data stored and transmitted by the device, to supply chain management, penetration testing and vulnerability reporting programs. Further principles outline the requirement for life-cycle security patching.
- **User Access & Credentials** (13-17) – Requirement of encryption of all passwords and user names, shipment of devices with unique passwords, implementation of generally accepted password re-set processes and integration of mechanisms to help prevent "brute" force login attempts.
- **Privacy, Disclosures & Transparency** (18-33) – Requirements consistent with generally accepted privacy principles including prominent disclosures on packaging, point of sale and/or posted on line, capability for users to having the ability to reset devices to factory settings and compliance with applicable regulatory requirements including the EU GDPR and children's privacy regulations. Required disclosures on the impact to product features or functionality if connectivity is disabled.
- **Notifications & Related Best Practices** (34-40) - Key to maintaining device security is having mechanisms and processes to promptly notify a user of threats and action(s) required. Principles include requiring email authentication for security notifications and that messages must be communicated clearly for users of all reading levels. In addition, tamper-proof packaging and accessibility requirements are highlighted.

IoT Trust Framework ● **Required (Must)** ○ **Recommended (Should)**	
Security – Device, Apps and Cloud Services	
1. Disclose whether the device is capable of receiving security related updates and if yes, disclose if the device can receive security updates automatically and what user action is required to ensure the device is updated correctly and in a timely fashion.	●
2. 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.	●
3. All IoT support web sites must fully encrypt the user session, from the device to the backend services. Current best practices include HTTPS and 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.[1]	●
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 penetration tests at least semi-annually.[2]	●
5. 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.	●
6. Ensure a mechanism is in place 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 including but not limited to signing and integrity checking.	●
7. Updates and patches must not modify user-configured preferences, security, and/or privacy settings without user notification. In cases where the device firmware or software is overwritten, on first use the user must be provided the ability to review and select privacy settings.	●
8. Security update process must disclose if they are Automated (vs automatic). Automated updates provide users the ability to approve, authorize or reject updates. In certain use cases a user may want the ability of deciding how and when the updates are made including but not limited to data consumption and connection through their mobile carrier or ISP connection. Conversely automatic updates are pushed to the device seamlessly without user interaction and may or may not provide user notice.	●

9. Ensure all IoT devices and associated software, have been subjected to a rigorous, standardized software development lifecycle testing including unit, system, acceptance, and regression testing and threat modeling, along with maintaining an inventory of the source for any third party/open source code and/or components. Employ generally accepted code and system hardening techniques across a range of typical use case scenarios, 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 current software and/or on first boot push automatic updates to address any known critical vulnerabilities.	●
10. Conduct security, and compliance risk assessments for all service and cloud providers. See IoT resource guide https://otalliance.org/IoT	●
11. Develop and maintain a "bill of materials" including software, firmware, hardware and third-party software libraries (including open source modules and plug ins). (This applies to the device, mobile and cloud services to help quickly remediate reported vulnerabilities.)	○
12. Design devices to minimum requirements necessary 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	
13. 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.	●
14. 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.	●
15. 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.	●
16. Provide users notification of password reset or change utilizing secure authentication and /or out-of-band notice(s).	●
17. 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	
18. 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, user friendly short URLs and other similar methods at point-of-sale.	●
19. Disclose the duration and end-of-life security and patch support, (beyond product warranty). Support may end on a sunset date, such as January 1, 2025 or for a specific duration from time of purchase not unlike a traditional warranty. Ideally such disclosures should be aligned to the expected lifespan of the device and communicated to the consumer prior to purchase. *(It is recognized IoT devices cannot be indefinitely secure and patchable. Consider communicating the risks of using a device beyond its usability date, and impact and risk to others if warnings are ignored or the device is not retired).* If users must pay any fees or subscribe to an annual support agreement this should be disclosed prior to purchase.	●
20. 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.	●

21. 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. Include what happens when the device no longer receives security updates or if the user fails to update the device. *(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).*	●
22. Disclose the data retention policy and storage duration of personally identifiable information.	●
23. IoT devices must provide notice and/or request a user confirmation when initially pairing, onboarding, and/or connecting with other devices, platforms or services.	●
24. 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).	●
25. 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.	●
26. 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."	●
27. 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.	●
28. 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.	●
29. 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.	●
30. 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.[3] [4]	●
31. 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.	●
32. 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.	○
33. Provide the ability to reset a device and application to factory settings, providing the ability for erasure of user data in the event of transfer, rentals, loss or sale.	○

Notifications & Related Best Practices	
34. 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.[5]	●
35. For email communications within 180 days of publishing a DMARC policy, implement a reject or quarantine policy, helping ISPs and receiving networks to reject email which fails email authentication verification checks.[6]	○
36. IoT vendors using email communication are recommended to adopt transport-level confidentiality including generally accepted security techniques to aid in securing communications and enhancing the privacy and integrity of the message. (Also referred to as "Opportunistic TLS for email".[7]	○
37. 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 in a compromised state.	○
38. 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.	○
39. 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).	●
40. Enact a breach and cyber response and consumer notification plan to be re-evaluated, tested and updated at least annually and/or after significant internal system, technical and/or operational changes.	●

Resources and updates are posted at https://otalliance.org/IoT

Terminology, Definitions & Clarifications

1. Scope - Focused on "consumer grade devices and services for the home, enterprise including wearable technologies. Smart Cars including autonomous, self-driving vehicles as well as medical devices and HIPAA data[8] are beyond the scope of the Framework, yet the majority of the criteria are deemed to be applicable. Respectively they fall under regulatory oversight of the National Highway Traffic Safety Administration (NHTSA) and the Food and Drug Administration, (FDA). [9]
2. The terms device manufacturers, vendors, application developers, service providers and platform operators are all indicated by the term "Companies."
3. It is expected companies disclose instances 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.

[1] https://otalliance.org/resources/always-ssl-aossl

[2] https://otalliance.org/blog/responsible-coordinated-ethical-vulnerability-disclosures

[3] Companies, products and services must be in compliance with any law or regulation of the jurisdiction that governs their collection and handling of personal and sensitive information, including but not limited to the adherence to the EU-US Privacy Shield Framework www.commerce.gov/privacyshield and/or the EU General Data Protection Regulation (GDPR) www.eugdpr.org. Failure to comply may constitute non-compliance with this framework.

[4] COPPA https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule

[5] Email Authentication - https://otalliance.org/eauth

[6] DMARC -https://otalliance.org/resources/dmarc

[7] TLS for Email - https://otalliance.org/best-practices/transport-layered-security-tls-email

[8] U.S. Department of Health & Human Services, Health Information Privacy http://www.hhs.gov/hipaa/index.html

[9] http://www.nhtsa.gov/Vehicle+Safety and http://www.fda.gov/MedicalDevices/default.htm

OTA is an initiative within the Internet Society (ISOC), a 501c3 charitable non-profit with the mission to promote the open development, evolution, and use of the Internet for the benefit of all people throughout the world. OTA's mission is to enhance online trust, user empowerment and innovation through convening multi-stakeholder initiatives, developing and promoting best practices, responsible privacy practices and data stewardship. To learn more visit https://otalliance.org and https://www.internetsociety.org.

r622