物联网保安与私隐保密的信任框架（2.5 版）

IoT Trust Framework® 中有一套战略原则，在物联网设备的货运过程及其整个生命周期中，这些原则是进一步保护物联网设备及其数据所必需的。对于已连网的家庭、办公室和可穿戴技术，包括玩具、活动跟踪装置和健身设备，已经通过以达成共识为导向的多利益相关者流程确定标准。此框架大致说明了必须在购买产品之前提供的全面公开信息，数据收集相关政策、使用情况和披露情况，以及保质过期后的保安修补条款和条件。发现漏洞以及发出攻击后，对于尽可能使物联网设备的保护更加严密，保安更新不可或缺。此外，有关设备更新难度和某些数据保密相关问题，对于要提高透明度并改善沟通效果的制造商，此框架中还有一些建议。

处理固有保安风险和保密问题时，最重要的就是在整个设备解决方案或生态系统中实施相关原则。这些原则涵盖设备、传感器、辅助应用程序，以及終端/云服务。随着许多依赖于第三方或开源部件和软件的产品的上市，开发人员有义务实施这些原则并进行供应链保安和保密的风险评估。

作为开发人员、采购人员和零售人员的风险评估指南，此框架是未来物联网认证计划的基础。揭示符合这些标准的设备，从而帮助消费者及公共部门和私营产业作出知情的购买决策，这就是 OTA 的目标。此框架及相关资源可在 https://otalliance.org/IoT 中获得。

此框架分为 4 个主要部分：

- **保安原则** (1-12) – 适用于任何设备或传感器，以及所有应用程序和終端云服务。这些原则涵盖严格的软件开发保安流程的实施，有关由设备存储和传输的数据的数据保安原则，以及供应链管理、渗透测试和漏洞报告计划。其他原则概括的是终身保安修补要求。
- **用户访问和凭据** (13-17) – 对所有口令和用户名称加密的要求，有唯一口令的设备的货运，普遍接受的口令重置流程的实施，以及为了防止尝试“暴力”登录而进行的机制一体化。
- **私隐保密、公开信息和透明度** (18-33) – 与普遍接受的保密原则一致的要求，包括包装上、销售点和/或在线公布的醒目的公开信息，用户用于将设备设置重置为出厂设置的功能，以及适用监管要求（包括 歐盟通用資料保護規則和儿童隐私条例）的遵从程度。也包括有关禁止连接后对产品特性或功能的影响的公开信息。

- **通知和相关最佳做法** (34-40) - 保持设备安全无虞的关键，是有用于针对威胁和所需采取的行动迅速通知用户的机制和流程。原则包括对安保通知要求进行电子邮件身份验证，以及必须向阅读水平各异的用户清楚地传递消息。此外，还强调了防篡改包装和易用性要求。

IoT Trust Framework ● 要求遵循（必须遵循） O 建议遵循（应该遵循）	
保安– 设备、应用和云服务	
1. 说明设备能否接收安保相关更新，如果能，则说明设备能否自动接收保安更新，以及用户必须采取什么行动才能确保设备正确及时地得到更新。	●
2. 确保设备及相关应用程序支持普遍接受的最新安保和密码协议及最佳做法。对于传输和存储的所有个人身份信息，都必须已经按普遍接受的最新保安标准加密。这包括但不限于有线、Wi-Fi 和蓝牙连接。	●
3. 对于从设备到終端服务的用户会话，所有物联网支持网站都必须进行全面加密。当前最佳做法包括默认情况下实施 HTTPS 和 HTTP 严格传输安保 (HSTS) 机制，也称为 AOSSL 或“始终使用 SSL”。设备中必须有用于对其終端服务和辅助应用程序进行可靠身份验证的机制。[1]	●
4. 物联网支持站点必须实施定期监控，并且不断改善站点保安和服务器配置，以使漏洞的影响减小到可以接受的程度。至少每半年进行一次渗透测试。[2]	●
5. 建立协调一致的漏洞公开机制，包括用于对第三方（包括但不限于客户、消费者、学术界和研究团体）外来漏洞报告进行接收、跟踪和迅速反应的流程和系统。通过远程更新和/或通过可操作的消费者通知或其他有效机制，以对公众负责的方式，对产品发布后发现的设计漏洞和威胁进行补救。开发人员必须考虑实施"报告缺陷的奖赏"计划，并且以众包的方式征集方法，以便进一步查明漏洞。	●
6. 确保自动化安全和保障方法机制已经就绪，以提供软件和/或固件更新、修补程序和修订版本。这些更新必须有签名并且/或者以其他方式验证，证实其来自可靠的来源，包括但不限于签名和完整性检查。	●
7. 未得到用户通知的情况下，更新和修补程序不得修改用户配置的偏好、安保和/或密保设置。如果设备固件或软件已被覆盖，则必须在用户首次使用时使其能够审核和选择密保设置。	●
8. 如果保安更新流程是自动化（而不是自动）流程，则必须公开这些流程。通过自动化更新，用户能够对更新进行审批、授权或拒绝。某些情况下，用户可能需要决定更新方式和更新时间的能力，包括但不限于通过其移动运营商或 ISP 连接使用数据及建立连接。相反，自动更新却是畅通无阻地向设备推送的更新，没有用户互动，并且未必会向用户发出通知。	●

9. 确保所有物联网设备及相关软件都一直经过严格的标准化软件开发生命周期测试，包括单元测试、系统测试、接受度测试、回归测试、威胁建模，以及维持第三方/开源代码和/或部件来源的清单。在某些典型用例情形中运用普遍接受的代码和系统巩固技术，包括防止在设备、应用和云服务之间发生数据泄露。从项目开始到实施、测试和部署，都必须考虑安全保障，才能开发安全无虞的软件。设备必须与最新软件一同发运，并且/或者在首次引导时推送自动更新，以应对所有已知严重漏洞。	●
10. 对所有服务和云提供商执行安保和合规风险评估。请参见物联网资源指南：https://otalliance.org/IoT	●
11. 逐步编制并维持“材料清单”，包括软件、固件、硬件和第三方软件库（包括开源模块和插件）。这适用于设备、移动和云服务，以便对报告的漏洞迅速地进行补救。	○
12. 按运行所需符合的最低要求设计设备。例如，仅当 USB 端口或内存卡插槽是设备运行和维护所需的部件时，才添加这些部件。必须禁用未經使用的端口和服务。	●
用户访问和凭据	
13. 默认情况下添加强身份验证，包括提供唯一、系统生成或一次性口令，也可使用安保认证凭据。按需要求使用唯一的口令，用于管理访问操作，划出设备与服务之间的界限，以及描述各自的出厂设置重置影响。	●
14. 提供普遍接受的物联网应用程序恢复机制及支持密码和/或机制，以便在没有用户口令的情况下用多重验证和身份验证（电子邮件和电话等）进行凭据重置。	●
15. 采取措施防止进行“暴力”和/或其他滥用性登录尝试（例如，使用自动化登录机器人，等等），方法是次数合理的无效登录尝试过后锁定或禁用用户和设备支持帐户。	●
16. 通过安保身份验证和/或带外通知，就口令重置或更改向用户发出通知。	●
17. 身份验证凭据（包括但不限于用户口令）必须经过加盐、哈希处理和/或加密。应用于所有已存储好的凭据，以便进一步防止擅自访问和暴力攻击。	●
密保、公开信息和透明度	
18. 先确保保密、保安和支援政策轻易就能发现，一清二楚并且立即就能查看，然后再购买、激活、下载或注册。除了产品包装上和网站中的醒目位置，还建议各个公司使用二维码，易于使用的短 URL，以及在销售点使用其他类似方法。	●
19. 公开持续时间及报废时的安保措施和修补程序支持（产品质保范围之外）。支持可在日落日结束，如 2025 年 1 月 1 日，也可从购买之时起持续指定的时间，不同于传统质保。理想情况下，这种公开必须以设备预期使用寿命为准，并在购买之前告诉消费者。*（物联网设备不能无限期地安全无虞并且能够修补，这是一个共识）。要考虑说明超期使用设备的风险，以及忽略警告或设备未淘汰对别人的影响和风险）。*如果用户必须为一年期支持协议付费或订购，则必须在购买之前公开这一情况。	●

20. 大张旗鼓地公开收集了什么个人身份信息及敏感数据类型和特征，以及其使用方式，从而以对于相应功能用途合理的数据，以及数据收集目的限制收集范围。对于所有其他目的，要公开并且让消费者选择是否参与。	●
21. 公开什么功能会在连接或終端服务禁用或停止后不起作用，以及如何失去效用，包括但不限于对实体保安的潜在影响。要包括设备得不到安全更新或用户不更新设备时会发生什么情况。*（一方面，要考虑用内置控件禁止连接或禁用端口，以减小潜在威胁，另一方面，要根据设备使用情况维持核心产品功能，从而抵消潜在使用寿命/安全问题的影响）。*	●
22. 公开个人身份信息的数据保留政策和存储持续时间。	●
23. 开始与其他设备平台或服务配对、交换信息和/或连接时，物联网设备必须发出通知并且/或者要求用户确认。	●
24. 公开物联网设备/产品/服务所有权和数据是否可以及怎样才能转让（例如，已连网的住宅即将卖给新业主，或者健身跟踪装置的出售）。	●
25. 仅在消费者已同意的情况下将消费者的个人数据透露给第三方，除非需要为产品功能的使用或服务运营透露，并且以产品功能使用和服务运营为限。要求第三方服务提供商遵守同样的政策，包括对此类数据保密，以及所有数据丢失/泄露事故和/或擅自访问行为的通知要求。	●
26. 提供控制权和/或文档，从而使消费者能够查看和编辑物联网设备密保偏好，包括将设置重置为"出厂默认设置"的功能。	●
27. 承诺不出售或转让所有消费者身份数据，除非这些数据是起初用于收集这些数据的核心业务的出售或清算所依赖的数据，前提是收购方保密政策中的相关条款没有重大变动。否则必须得到通知和许可。	●
28. 向消费者提供查看运营前说明的密保做法后免费退回产品的功能，前提是此类条款未在购买之前大张旗鼓地公开。退回产品的期限（天数）必须与最新零售商换货政策一致或事先详细说明。	●
29. 每当提供拒绝或退出政策的机会时，必须清楚而客观地说明后果，包括对产品特性或功能产生的影响。建议将最终用户参与和/或披露数据的重要性告诉最终用户。	●
30. 遵守适用条例，包括但不限于《儿童在线隐私保护法》(COPPA) 和国际保密、保安和数据传输监管要求。[3] [4]	●
31. 至少要公开发布两年的重大政策通知变动历史记录。最佳做法包括加盖日期戳，用红线勾销，以及总结变动的影响。	●
32. 向用户或代理人提供停止使用、丢失或出售设备时删除或匿名化存储在公司服务器中的个人或敏感数据（除了购买交易历史记录）的功能。	○
33. 提供将设备和应用程序设置重置为出厂设置的功能，包括转让、出租、丢失或出售时删除用户数据的功能。	○

通知和相关最佳做法	
34. 必须对最终用户通信内容（包括但不只限于电子邮件和短信）采用身份验证协议，以便进一步防止遭到鱼叉式网络钓鱼和欺骗攻击。对于域，必须对所有保安和保密相关通信内容和通知，以及已暂停的域和从未用于发送电子邮件的域实施 SPF、DKIM 和 DMARC。[5]	●
35. 对于电子邮件通信，在公布 DMARC 政策后的 180 天内，要实施拒绝或隔离政策，这有助于 ISP 和接收网络拒绝未能通过电子邮件身份验证检查的电子邮件。[6]	O
36. 进行电子邮件通信的物联网厂商必须在传输层面保密，包括使用普遍接受的保安技术，以便进一步保护通信内容并提高消息的私密性和完整性（也称为“用于电子邮件的投机性 TLS”）。[7]	O
37. 采取措施进一步防止或揭露设备实体篡改行为。此类措施有助于防止设备安装后遭到恶意打开或修改，或防止设备在退给零售商时处于已受损状态。	O
38. 要考虑如何顾及可能有视力障碍、听力障碍或行动障碍的用户的辅助功能要求，以便尽可能使用户能够轻易使用所有实体功能。	O
39. 逐步编写通信流程，以便尽可能提高用户对所有潜在保安问题、保密问题、报废通知和潜在产品召回（包括应用内通知）的认知度。撰写信件时，必须尽可能按普通用户的阅读水平提高用户的理解程度。认识到英语可能是用户的“第二语言”后，要考虑撰写多语言信件（请参见有关安保和消息完整性的原则）。	●
40. 制定违规行为和网络攻击响应和消费者通知计划，至少每年将其重新评估、测试和更新一次，并且/或者在重大内部系统、技术和/或运营变动发生后对其进行重新评估、测试和更新。	●

资源和更新发布在：https://otalliance.org/IoT

术语、定义和详细说明

1. 范围 - 专注于“适用于家庭和企业（包括可穿戴技术）的消费级设备和服务”。智能汽车（包括自主的自动驾驶车辆）及医疗器械和 HIPAA 数据[8]不在此框架涵盖范围内，但大多数标准已被视为适用标准。二者分别归美国国家公路交通安全管理局 (NHTSA) 和美国食品药品监督管理局 (FDA) 监管。[9]
2. 词语“设备制造商”、“厂商”、“应用程序开发商”、“服务提供商”和“平台运营商”都用“公司”一词指代。
3. 公司预计会向执法部门公开数据披露事例，并将任何适用透明度报告说成是法律允许披露的报告。
4. 智能设备是指已连网并且只能进行单向通信的设备（和传感器）。

[1] https://otalliance.org/resources/always-ssl-aossl
[2] https://otalliance.org/blog/responsible-coordinated-ethical-vulnerability-disclosures
[3] 公司、产品和服务必须合乎用于治理其个人和敏感信息收集和处理的司法辖区的法律或条例，包括但不限于遵循《欧美隐私盾框架》(www.commerce.gov/privacyshield)，以及/或者《欧盟数据保护条例》(GDPR) (www.eugdpr.org)。不遵守可能会构成不遵从此框架的行为。
[4] COPPA https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/childrens-online-privacy-protection-rule
[5] 电子邮件通知 - https://otalliance.org/eauth
[6] DMARC -https://otalliance.org/resources/dmarc
[7] 用于电子邮件的 TLS - https://otalliance.org/best-practices/transport-layered-security-tls-email
[8] 美国 卫生与公众服务部健康状况信息保密司 http://www.hhs.gov/hipaa/index.html
[9] http://www.nhtsa.gov/Vehicle+Safety 和 http://www.fda.gov/MedicalDevices/default.htm

OTA 是在 Internet Society (ISOC) 内部实施的计划，而后者是 a 501c3 慈善非营利组织，其使命是促进海纳百川式的发展壮大，以及为使全世界人民受益而使用因特网。OTA 的使命是通过召集大家实施多利益相关者计划，逐步构想最佳做法和负责任的密保做法，并促进这些做法的采用和数据管理工作，来提高在线信任度，加大对用户的帮助力度，以及改善创新工作。要了解详情，请访问 https://otalliance.org 和 https://www.internetsociety.org。

R1014