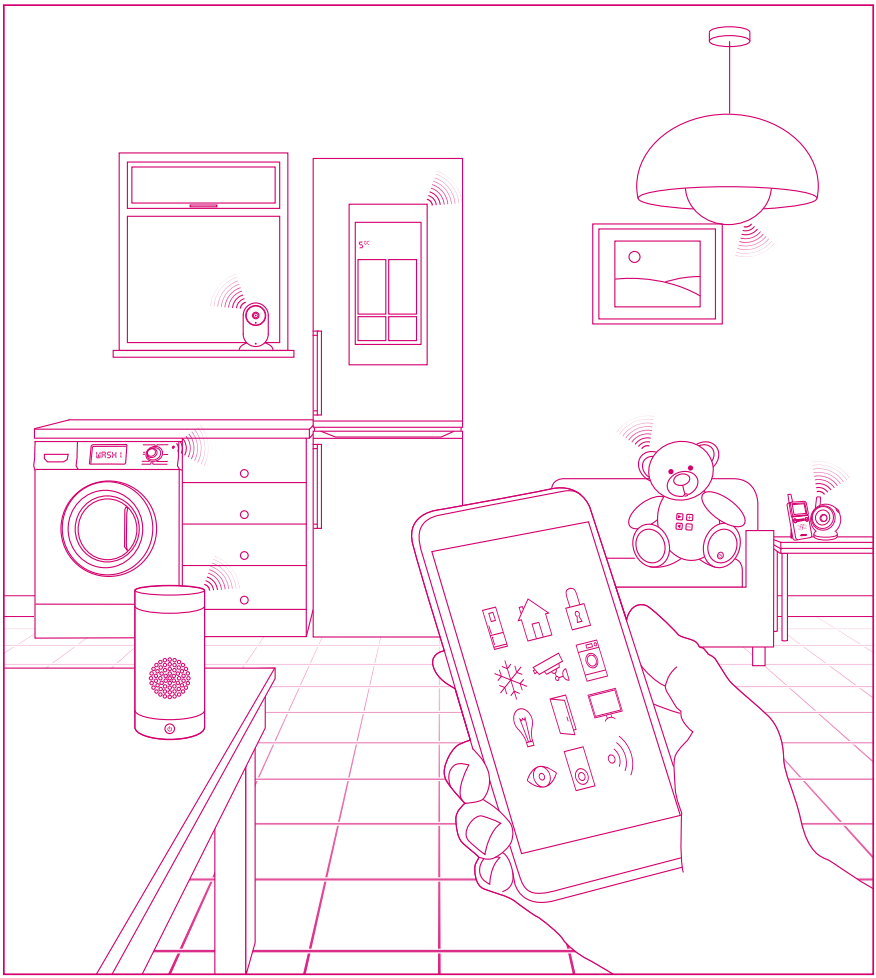
Department for
Digital, Culture,
Media & Sport

消费类物联网设备安全行为准则



2018 年 10 月

执行摘要

随着人们将家中越来越多的设备连接至互联网，传统上一直脱机使用的产品和设备现在也成为了“物联网”(IoT) 的一部分。

科技在家居生活中的比重越来越高，而 IoT 为此开启了新篇章，让人们的生活更轻松愉悦。人们传输到联机设备和服务的个人数据与日俱增，因此当今保证这些产品的网络安全就像保证我们的家庭安全一样重要。

本行为准则旨在制订一系列准则，以支持所有涉及消费类 IoT 开发、制造和零售的各方，竭力确保产品采用安全设计，让人们能更轻松地在数字世界中保持安全。

本行为准则包含了 13 条以结果为导向的准则，均属于获得广泛认可的 IoT 安全保障最佳做法。本行为准则由英国数字、文化、传媒和体育部 (DCMS) 与英国国家网络安全中心 (NCSC) 联合制定，接受了行业、消费者协会和学术机构的指导。该准则最初于 2018 年 3 月作为《安全设计》报告的一部分以草案形式发布。[1]

[1] DCMS，2018，‘Secure by Design: Improving the cyber security of consumer Internet of Things: Report’（《安全设计：改善消费类物联网设备的网络安全：报告》），https://www.gov.uk/government/publications/secure-by-design

简介

物联网 (IoT) 为人们带来了巨大的机会。但我们也发现，当今市场上的很多设备缺少基本的安全措施。人们应该能够从连接技术中安全地获益，并确保具备充足的安全和隐私保护措施来保护他们的在线活动。

本行为准则为 IoT 制造商和其他行业利益相关者制定了实用步骤，以改进消费类 IoT 产品及其相关服务的安全性。实施这 13 条准则有助于保护消费者的隐私和安全，同时使消费者更能安全地使用他们的产品。它还可以减少从不安全的 IoT 设备和服务启动的分布式拒绝服务 (DDoS) 攻击的威胁。

这些准则整合了 IoT 安全保护方面公认的良好做法。它们注重结果，而不是规范，让组织能够灵活地创新和实施适合其产品的安全解决方案。

本行为准则并非解决所有安全挑战的良方。只有转变为以安全为先的思维模式，并投资于安全开发生命周期，才能保证组织成功创建安全的 IoT。从产品开发到整个生命周期，产品和服务的设计应始终注重安全性。组织还应定期评估与其产品和服务相关的网络安全风险，并实施适当的措施加以应对。

IoT 产品的供应链可能高度复杂，可能具有国际化的特点，往往涉及到多家组件制造商和服务提供商。该准则的目的是在整个供应链中倡导和促进积极的安全转型。

许多行业团体和国际论坛都在为 IoT 制定安全建议和标准。[2]这份行为准则旨在补充和支持这些工作以及已发布的相关网络安全标准。本行为准则直接与行业合作制定，我们希望未来与消费类 IoT 相关的保证和信任标识方案也能与本准则保持一致。

实施该行为准则可帮助组织遵守适用的数据保护法律。例如，欧盟通用数据保护法规 (GDPR) 要求安全地处理个人数据。[3]

[2] PETRAS, 2018, 'Summary literature review of industry recommendations and international developments on IoT security'（《关于 IoT 安全的行业建议和国际发展的文献综述》）, https://www.gov.uk/government/publications/secure-by-design

[3] GDPR 的第 5(1)(f) 条款提到了个人数据的“完整性和机密性”

实施

本行为准则基于一个映射文档，该文档可将每条准则都链接至主要行业标准、建议和指导。本文档为行为准则中的十三条准则提供了更多背景，并有助于行业实施这些准则。此文档还显示了该准则与在整个全球组织内执行的 IoT 安全工作之间的关系。

优先级和结构

前三条准则需要优先考虑，因为默认的密码、漏洞披露和安全更新将在短期内带来最大的安全优势。

支持文本阐明了基本原理，并为每条准则添加了进一步的解释。文档末尾的附加注释回答了常见问题。

受众

每条准则都指出了负责其实施的主要利益相关者。利益相关者的定义是：

设备制造商 – 创建组装好的最终联网产品的实体。最终产品可能包含许多其他制造商的产品。

IoT 服务提供商 – 提供诸如网络、云存储和数据传输等服务（作为 IoT 解决方案的一部分）的公司。联网设备可能作为服务的一部分提供。

移动应用程序开发人员 – 开发和提供在移动设备上运行的应用程序的实体。这些通常作为 IoT 解决方案的一部分，通过与设备交互的方式进行提供。

零售商 – 面向消费者的接入网络产品和相关服务的卖方。

[4] DCMS, 2018, 'Mapping of IoT Security Recommendations, Guidance and Standards to the Code of Practice for Consumer IoT Security'（《IoT 安全建议、指导和标准与《消费者物联网安全行为准则》之间的映射》）https://www.gov.uk/government/publications/secure-by-design

术语

术语“安全敏感数据”的使用旨在区分其他类型的敏感数据，例如 GDPR 中定义的特殊类别数据（正式名称为“敏感个人数据”）。安全敏感数据可能包括加密初始化向量。

术语“消费者”一词的使用是为了保持一致性；消费者通常被视为 IoT 产品和服务的最终用户。

适用范围

本行为准则适用于连接到互联网和/或家庭网络和相关服务的消费类 IoT 产品。非详尽的示例列表包括：

- 联网的儿童玩具和婴儿监控器；
- 联网的安全相关产品，例如烟雾探测器和门锁；
- 智能摄像机、电视和扬声器；
- 可穿戴式健康跟踪器；
- 联网的家庭自动化和报警系统；
- 联网设备（例如洗衣机、冰箱）；
- 智能家庭助理。

相关服务是指与 IoT 设备连接的数字服务，例如移动应用程序、云计算/存储和第三方应用程序编程接口 (API) 等服务。

评论

英国数字、文化、传媒和体育部部将定期查看准则和发布更新，至少每两年一次。请联系 securebydesign@culture.gov.uk 获取通知。

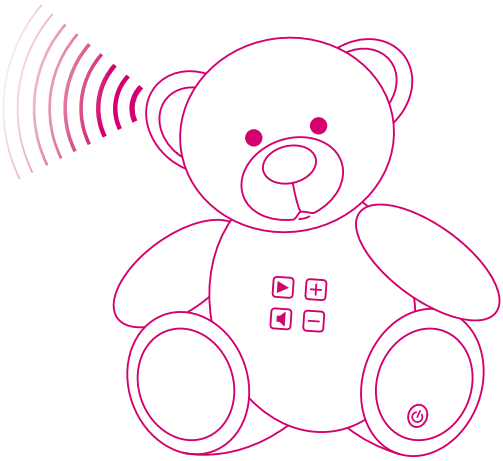
准则

1) 禁止使用默认密码

所有 IoT 设备密码都应是唯一的，并且不能重置为任何通用出厂默认值。

许多 IoT 设备在销售时使用的是通用默认用户名和密码（如“Admin，Admin”），消费者应对其进行更改。这是 IoT 中许多安全问题的源头所在，需要杜绝这种做法。应遵循密码和其他身份验证方法的最佳做法。[5]

主要适用于：
设备制造商



[5] 有关准则，请参阅：NCSC，2016，‘Password Guidance: Simplifying Your Approach’（《密码指导：简化您的方法》）https://www.ncsc.gov.uk/guidance/password-guidance-simplifying-your-approach。另请参阅：NIST，2017，‘NIST Special Publication 800-63B: Digital Identity Guidelines - Authentication and Lifecycle Management’（《NIST 特殊出版物 800-63B：数字身份指南 - 身份验证和生命周期管理》）https://pages.nist.gov/800-63-3/sp800-63b.html#sec5

2) 实施漏洞披露政策

作为漏洞披露政策的一部分，所有提供互联网连接设备和服务的公司都应提供公共联络点，以便安全研究人员和其他人能够报告问题。已披露的漏洞应及时予以处理。

了解安全漏洞使公司能够作出回应。作为产品安全生命周期的一部分，公司还应持续监视、识别和纠正其自身产品和服务中的安全漏洞。最开始就应直接向受影响的利益相关者报告漏洞。如果无法做到，则可向国家当局报告这些漏洞。[6] 有关在不同情况下应采取的不同做法的详细信息，请参阅注释。我们还鼓励公司与主管行业团体分享信息。[7]

主要适用于：
设备制造商
IoT 服务提供商
移动应用程序开发人员

[6] 在英国，漏洞报告可发送至 https://www.ncsc.gov.uk/contact
[7] 主管行业团体包括全球移动通信系统联盟 (GSMA) 和 IoT 安全基金会。可从 IoT 安全基金会获得有关协同漏洞披露的指导，该基金会在漏洞披露中引用了 ISO/IEC 29147 标准。可访问 https://www.gsma.com/cvd 查阅 GSMA 的行业级协同漏洞披露计划

3) 保持软件更新

联网设备中的软件组件应能够安全地执行更新。更新需及时进行，并且不能影响设备的功能。终端设备应发布一项寿命终止政策，该政策需明确规定设备接收软件更新的最短时间长度，以及采用该支持周期长度的原因。每次更新的需求都应清楚地向消费者提出，并且要易于实施。对于无法执行物理更新的受限设备，产品应可以隔离和更换。

还应保证安全补丁来源的可靠性，并通过安全的渠道交付。更新过程中应尽可能保证设备的基本功能继续运行，例如手表应继续显示时间、自动调温器应继续运行、锁应继续正常解锁和闭合。这似乎主要是设计方面的问题，但如果不考虑或未正确管理，可能会为某些类型的设备和系统带来重大安全问题。

软件更新应在设备销售后提供，然后在规定的周期内推送至该设备。购买产品时，应向消费者明确说明软件更新支持的周期。零售商和/或制造商应向消费者发出更新通知。对于不可能进行软件更新的受限设备，应明确指出更换支持的条件和周期。

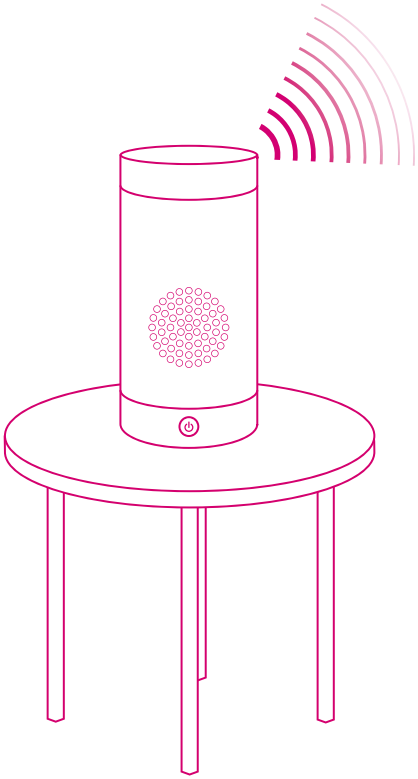
主要适用于：
设备制造商
IoT 服务提供商
移动应用程序开发人员

4) 安全存储凭据和安全敏感数据

任何凭证都应安全地存储在服务和设备上。不得使用硬编码在设备软件中的凭证。

设备和应用程序的逆向工程可轻松发现硬编码在软件中的凭证，诸如用户名和密码等。用于掩盖或加密这种硬编码信息的简单模糊处理方法也可能会受到破坏。安全敏感数据（例如加密密钥、设备标识符和初始化向量）应安全地存储。应使用安全、可信的存储机制，如受信任的执行环境以及相关的可靠、安全的存储所提供的存储机制。

主要适用于：
设备制造商
IoT 服务提供商
移动应用程序开发人员



5) 安全通信

安全敏感数据（包括所有远程管理和控制数据）在传输过程中应该采用适用于技术和使用方式属性的方法进行加密。所有密钥都应安全管理。

我们强烈鼓励应用开放、同行评审的互联网标准。

主要适用于：
设备制造商
IoT 服务提供商
移动应用程序开发人员

6) 尽量减少暴露的攻击面

所有设备和服务都应基于“最小权限原则”运行；未使用的端口应关闭，硬件不得提供不必要的访问权限，服务在未使用时应不可用，并应尽量减少代码，仅保留使服务正常运行所需的最少代码。软件应以适当的权限运行，同时考虑安全性和功能。

与其他任何应用领域一样，在 IoT 领域中，最小权限原则也是良好安全工程设计的基础。

主要适用于：
设备制造商
IoT 服务提供商

7) 确保软件完整性

应使用安全启动机制验证 IoT 设备上的软件。如果检测到未经授权的更改，设备应向用户/管理员发出警报，提醒其注意问题，并且除了执行警报功能所需的网络之外，不能连接到更广泛的网络。

从此类情况下执行远程恢复的能力应依赖于已知良好状态，例如在本地存储已知良好的版本，以实现设备安全恢复和更新。这将避免拒绝服务和成本高昂的召回或维护访问，同时管理设备被攻击者通过破坏更新或其他网络通信机制的方式进行接管的潜在风险。

主要适用于：
设备制造商

8) 确保个人数据受到保护

设备和/或服务处理个人数据时应遵循适用的数据保护法律，如《一般数据保护条例》(GDPR) 和《2018 年数据保护法案》。在每种设备和服务中，设备制造商和 IoT 服务提供商都应向消费者提供清晰、透明的信息，说明其个人数据的使用方式、使用者以及使用目的。这也适用于可能涉及的任何第三方（包括广告商）。如果个人数据依据消费者的授权进行处理，则此授权应以合法、有效的方式获得，并允许消费者随时撤回。

此准则可确保：

i. IoT 制造商、服务提供商和应用程序开发人员在开发和交付产品和服务时遵守数据保护义务；

ii. 根据数据保护法律处理个人数据；

iii. 协助用户确保其产品的数据处理操作一致，并且根据规范正常运行；

iv. 为用户提供通过适当配置设备和服务功能来保护其隐私的方法。

主要适用于：
设备制造商
IoT 服务提供商
移动应用程序开发人员
零售商

9) 使系统能从故障中迅速恢复

考虑到存在数据网络中断或电力中断的可能性，根据 IoT 设备和服务的用途或依赖于其的系统，如果 IoT 设备和服务需要具备恢复机制，则应具备相应的内置恢复机制。IoT 服务应尽可能在网络断开的情况下保持正常工作能力、可在本地正常运行，并应在恢复供电时完全恢复。设备应能够以合理状态和有序的方式重新加入网络，而不是通过大规模重新连接的方式重新加入。

当今的消费者在一些日益重要的使用情形中依赖于 IoT 系统和设备，这些使用情形可能与安全相关或影响生命。如果发生网络断开，服务应保持在本地正常运行，这是一种可提高恢复能力的措施。其他措施可能包括构建冗余和对 DDoS 攻击的防范措施。应基于用途确定适当的恢复能力，同时要考虑到可能依赖于这些系统、服务或设备的其他人，因为其影响可能会比预期更广泛。

主要适用于：
设备制造商
IoT 服务提供商

10) 监控系统遥测数据

如果从 IoT 设备和服务收集遥测数据，如使用和测量数据，则应监控是否存在安全异常。

监控遥测数据（包括日志数据）有助于安全评估，并支持在早期发现异常情况，从而最大限度地降低安全风险，并快速缓解问题。但是，根据准则 8，应将对个人数据的处理量保持在最低限度，并向消费者说明要收集哪些数据及收集原因。

主要适用于：
IoT 服务提供商

11) 使用户能够轻松删除个人数据

设备和服务的设置应允许消费者在转让设备所有权、希望删除数据和/或想要处置设备时轻松删除个人数据。应向消费者提供有关如何删除其个人数据的明确说明。

IoT 设备可能会更换所有权、最终被回收或处置。可提供相应的机制，让消费者能够保持控制和删除服务、设备和应用程序中的个人数据。

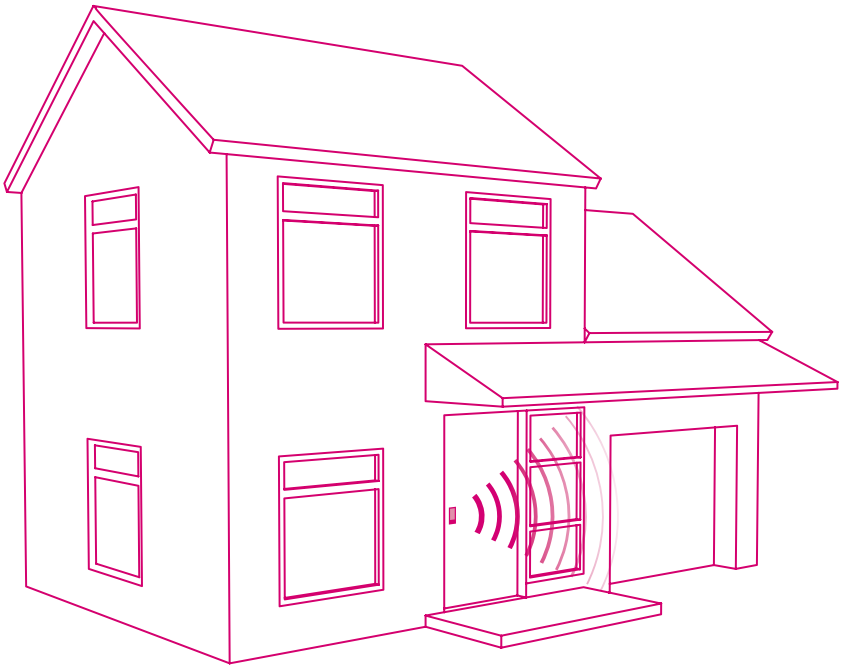
主要适用于：
设备制造商
IoT 服务提供商
移动应用程序开发人员

12) 轻松安装和维护设备

IoT 设备的安装和维护应采用最少的步骤，并应遵循安全最佳做法。还应向消费者提供有关如何安全地设置其设备的指导。

可通过是当地解决用户界面中的复杂性和改善设计来减少甚至消除由于消费者混淆或错误配置导致的安全问题。向用户提供有关如何安全地配置设备的指导，也可降低其受到威胁的可能性。

主要适用于：
设备制造商
IoT 服务提供商
移动应用程序开发人员



13) Validate input data

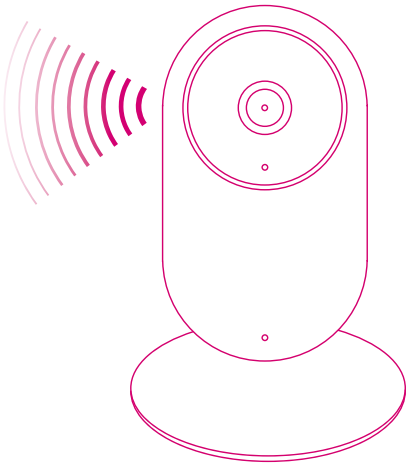
通过用户界面输入的数据，以及通过应用程序编程接口 (API) 传输的数据或在服务和设备之间的网络传输的数据均应执行验证。

格式设置不正确的数据或通过不同类型的接口传输的代码都可能破坏系统。攻击者通常采用自动化工具来利用未验证数据的潜在缺陷和弱点。示例包括但不限于以下类型的数据：

i. 不属于预期类型，例如可执行代码，而不是用户输入的文本。

ii. 超出范围，例如温度值超过传感器限值。

主要适用于：
设备制造商
IoT 服务提供商
移动应用程序开发人员



附加注释

准则 1 禁止使用默认密码: 尽管已经做了很多努力来消除对密码的依赖，提供对用户和系统进行身份验证的替代方法，但在目前推向市场的某些 IoT 产品中，仍在使用默认用户名和密码，这类密码涉及到从用户界面到网络协议的多个环节。这种做法是不可接受的，应停止使用。通过唯一和不可更改的身份，可以进一步加强设备安全性。

准则 2 协同漏洞披露 (CVD): CVD 是国际标准化组织 (ISO) 提出的一项标准，它实施简单，并且已在全球各地的多家大型软件公司中成功得到了验证。[8] 但是，CVD 仍未成为 IoT 行业所采纳的成熟标准，有些公司可能会对与安全研究人员打交道持谨慎态度。CVD 为安全研究人员提供了一种联系各公司的方法，以将安全问题通报给公司，从而使公司提前得知恶意攻击威胁，并让他们有机会在公开披露之前解决漏洞。

提供联网设备和服务的公司对可能会因其故障而遭受伤害的第三方负有提醒义务，并且应妥善制订 CVD 计划。此外，通过行业实体共享此信息的公司可以帮助受困于同样问题的其他人。

根据具体情况，可能需要采用不同的披露方法:

与单个产品或服务相关的漏洞: 问题应直接报告给受影响的利益相关者（例如设备制造商、IoT 服务提供商或移动应用程序开发人员）。这些报告的来源可能是安全研究机构或行业同行。如果与设备制造商或其他受影响的利益相关者联系后，他们不能及时采取行动，则可以直接向英国国家网络安全中心 (NCSC) 报告问题。

系统性漏洞: 如果设备制造商等利益相关者发现存在潜在的系统性问题，那么可能就要归入这种类型。尽管在设备制造商自己的产品中进行修复十分重要，但分享此信息也能对行业和消费者带来巨大的好处。同样，安全研究人员也可报告此类系统性漏洞。在这种情况下，相关的主管行业机构可以执行协调，应对更大规模的反响。NCSC 可以为主管行业机构提供建议和指导，以实现协调响应。

[8] 国际标准化组织 2014，‘ISO/IEC 29147 - Vulnerability Disclosure’（ISO/IEC 29147 - 漏洞披露），https://www.iso.org/standard/45170.html

根据具体事件的不同，针对漏洞的“及时处理”也会有所不同，根据约定俗成的标准，修复漏洞流程的时间不超过 90 天。硬件修复可能比软件修复的时间更长。此外，与服务器软件修复相比，必须部署到设备上的修复程序可能需要一定的时间来部署。

*准则 3 保持软件更新：*软件安全更新是公司为保护其客户和更广泛的技术生态系统，所能做到的最重要的事情之一。漏洞通常源于被视为与安全不相关的软件组件。因此，所有软件都应保持更新并得到良好的维护。通常，修复程序可以作为自动更新的一部分，采用预防性方式将推送至设备，可在安全漏洞被利用之前将其消除。这方面的管理可能高度复杂，尤其是在有云更新、设备更新和其他服务更新时。因此，明确的管理和部署计划至关重要，更新支持的当前状态应对消费者保持透明。

在许多情况下，发布软件更新将涉及到对其他组织的多个依赖方，例如子组件的制造商。这不能作为停止更新的理由 - 本行为准则的目的是鼓励在整个软件供应链中实施积极的安全变革。在一些情况下，设备无法修补设备。某些极度受限的设备就属于此类情况，对于这些设备，应制定更换计划，并将其清楚地传达给消费者。此计划应详述需要更换技术的时间，在适用情况下，还应详述硬件和软件支持的终止时间。

对于需要设备保持继续正常运行的消费者来说，这可能至关重要。这就是更新应该“尽可能不影响设备功能”的原因。在更新时，尤其是执行安全相关功能的设备不应完全关闭；应维持最基础的系统功能，例如加热系统或防盗报警系统。这些类型的设备的制造商还应考虑采用更具恢复能力的架构。

务必注意，软件更新机制本身也是一种攻击媒介，应确保其受到保护。

*准则 5 安全通信：*安全控制的适当性和加密的使用取决于许多因素，包括使用环境。[9] 由于安全性不断发展变化，很难提供有关加密措施的规范性建议，同时又保证这样的建议不会很快过时。实施者应确保其产品能够满足用户的需求，同时又能抵御针对加密机制的攻击。

[9] 可以参考 NCSC 等机构提供的指导信息，例如 NCSC 指导信息：
https://www.ncsc.gov.uk/guidance/tls-external-facing-services

*准则 7 确保软件完整性：*如果 IoT 设备检测到其软件发生异常，则需要通知相关负责人。在某些情况下，设备可使用管理模式 - 例如，室内自动调温器可能有一种用户模式可以防止其他设置被更改。在这些情况下，可以向管理员发出警报，因为该人员能够处理警报。

*准则 9 使系统从故障中迅速恢复：*此条准则的目的是确保 IoT 服务保持正常运行，因为消费者在生活中的方方面面越来越多地采用 IoT 设备，包括与人身安全相关的功能。例如，如果联网防盗门的网络连接断开，用户被锁在门外，就会影响人们的生活。另一个例子是由于针对云服务的 DDoS 攻击而导致家庭暖气系统关闭。有必要注意，还有其他安全相关的法规可能适用，但关键在于如何避免导致这些[问题]的中断。