物联网安全管理体系

认证技术规范

文件编号：CTS TBGL146-2026

版本号：B/2

受控状态： （ 受控 ）

编写：技术部

审核：张辉根

批准：周春阳

首次发布：2022-12-20 **首次实施：2022-12-20** **修订实施日期：20260423**

江西腾标认证有限公司

目录

前言

本文件旨在为组织（以下简称“组织”）建立、实施、维护和持续改进物联网安全管理体系（IOTMS）提供要求和指南。本文件采用PDCA（策划-实施-检查-改进）循环模式，与 ISO/IEC 27001:2022《信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求》 的高阶结构保持一致，并充分融合了 GB/T 37044-2018《信息安全技术 物联网安全参考模型及通用要求》 的特定行业要求。

本文件旨在为组织在基于ISO/IEC 27001:2022建立和实施信息安全管理体系的过程中，提供一套专门的物联网安全控制选择和实施指南。本文件的核心架构与ISO/IEC 27001:2022完全一致，组织可通过实施本文件，建立一个同时满足ISO/IEC 27001和GB/T 37044-2018要求的整合性管理体系。组织应首先建立满足ISO/IEC 27001要求的信息安全管理体系（ISMS），并在此基础上扩展物联网安全管理要求。

1. 范围

本文件规定了组织建立、实施、保持和持续改进 物联网安全管理体系 的要求。本文件适用于

1） 组织建立、实施、保持和改进 物联网安全管理体系 管理方针和目标；

2） 认证机构对组织进行物联网安全管理体系认证。

2. 规范性引用文件

下列文件对于本文件的应用必不可少。凡是注日期的引用文件，仅注日期的版本适用于本文件。凡是不注日期的引用文件，其最新版本（包括所有的修改单）适用于本文件。

- ISO/IEC 27000 信息技术 — 安全技术 — 信息安全管理体系 — 概述和词汇
- ISO/IEC 27001:2022 信息安全、网络安全和隐私保护 — 信息安全管理体系 — 要求
- ISO/IEC 27002:2022 信息安全、网络安全和隐私保护 — 信息安全控制
- GB/T 37044-2018 信息安全技术 物联网安全参考模型及通用要求

注：认证审核时引用文件的有效性以审核实施时现行有效的最新版本为准。

3. 术语和定义

ISO/IEC 27000、ISO/IEC 27001:2022界定的以及下列术语和定义适用于本文件。ISO和IEC在以下地址维护用于标准化的术语数据库：

- ISO在线浏览平台：https://www.iso.org/obp
- IEC电子百科：https://www.electropedia.org/

3.1 物联网

将感知设备、网络、计算系统等物理实体和信息系统相连接，实现信息交换和通信，以实现智能化识别、定位、跟踪、监控和管理的网络。

[来源：GB/T 37044-2018, 3.1]

3.2 物联网系统

由感知控制、网络通信、应用服务等组成的，实现物联网功能的系统。

[来源：GB/T 37044-2018, 3.2]

3.3 安全区

若干特定功能域或子域所对应的信息安全需求的集合，每一安全区因所包含的域或子域的功能目标不同而会有不同的信息安全防护需求侧重。

[来源：GB/T 37044-2018, 3.3]

3.4 感知终端

物联网中用于感知和采集环境信息或执行控制指令的设备，如传感器、RFID标签、摄像头、执行器等。

3.5 物联网网关

连接感知网络与通信网络的设备，负责协议转换、数据汇聚和转发。

3.6 系统生存周期

物联网系统从规划设计到废弃退出的完整过程，包括规划设计、开发建设、运维管理、废弃退出四个阶段。

[来源：GB/T 37044-2018, 5.3]

4. 组织环境

4.1 理解组织及其环境

组织应确定与其意图相关的，且影响其实现IOTMS预期结果能力的外部和内部事项。

- **外部因素**：适用的信息安全法律和法规（如《网络安全法》、《数据安全法》、《个人信息保护法》等）、监管机构要求（如网信办、工信部、数据局等）、行业标准与最佳实践、物联网特有的威胁（如感知终端物理攻击、网络协议攻击、数据泄露、供应链攻击）、客户对物联网安全的期望等。
- **内部因素**：组织的规模、治理结构、物联网系统的复杂程度与规模、感知终端的类型与数量、网络架构、数据敏感度、人员物联网安全技能与意识、以往物联网安全事件记录等。

4.2 理解相关方的需求和期望

组织应确定：

a) 与IOTMS有关的相关方；

b) 这些相关方的有关要求；

c) 哪些要求将通过IOTMS予以解决。

相关方包括但不限于：物联网系统用户、感知终端供应商、网络服务提供商、平台运营商、应用开发者、监管机构、员工、合作伙伴、认证机构、公众。

组织应建立、实施并保持程序，以识别相关方，并促其参与到与IOTMS相关的已识别的议题中。与相关方的沟通应为一个**持续的过程**。**组织应将促进相关方参与所产生的输出形成文件**。

4.3 确定IOTMS的范围

组织应确定IOTMS的边界及其适用性，以建立其范围。在确定范围时，组织应考虑：

a) 4.1中提到的外部和内部事项；

b) 4.2中提到的要求；

c) 组织实施的活动与其他组织实施的活动之间的接口和依赖关系（特别是与感知终端供应商、网络服务提供商、平台运营商之间的接口）。

范围应形成文件化信息并可用。

4.4 物联网安全管理体系（IOTMS）

4.4.1 组织应按照本标准的要求，建立、实施、保持和持续改进物联网安全管理体系，包括所需过程及其相互作用。

组织应确定物联网安全管理体系所需的过程及其在整个组织中的应用，且应：

a) 确定这些过程所需的输入和期望的输出；

b) 确定这些过程的顺序和相互作用；
c) 确定和应用所需的准则和方法（包括监视、测量和相关绩效指标），以确保这些过程的有效运行和控制；
d) 确定这些过程所需的资源并确保其可获得；
e) 分配这些过程的职责和权限；
f) 按照 6.1 的要求应对风险和机遇；
g) 评价这些过程，实施所需的变更，以确保实现这些过程的预期结果；
h) 改进过程和物联网安全管理体系。
4.4.2 在必要的范围和程度上，组织应：
a) 保持成文信息以支持过程运行；
b) 保留成文信息以确信其过程按策划进行。

5. 领导作用

5.1 领导作用和承诺

最高管理者应通过以下活动，证实其在对IOTMS的领导作用和承诺：
a) 确保建立物联网安全方针和目标，并与组织战略方向一致；
b) 确保将IOTMS要求融入组织的业务过程；
c) 确保IOTMS所需的资源可获得；
d) 沟通有效的物联网安全管理的重要性；
e) 确保IOTMS达成其预期结果（如物联网系统安全、合规、客户信任）；
f) 指导并支持相关人员为IOTMS的有效性做出贡献；
g) 促进持续改进；
h) 支持其他相关管理角色在其职责范围内发挥领导作用。

5.2 方针

最高管理者应建立物联网安全方针，该方针应：
a) 与组织的宗旨相适宜；
b) 包括信息安全目标（见6.2）或为设定信息安全目标提供框架；
c) 包括对满足适用物联网安全相关要求的承诺；
d) 包括对持续改进IOTMS的承诺；
e) **特别应包括对保护物联网系统及其数据的保密性、完整性、可用性，以及遵守物联网安全法律法规的承诺**。
物联网安全方针应：
f) 形成文件化信息并可获取；
g) 在组织内得到沟通；
h) 适当时，可被相关方获取（如监管机构、客户）。

5.3 组织的岗位、职责和权限

最高管理者应确保与物联网安全相关岗位、职责和权限在组织内得到分配和沟通。

最高管理者应**指定一名或多名管理者**（如物联网安全负责人、信息安全负责人），不论其是否负有其他职责，应使其具有以下方面的岗位、职责和权限：

a) 确保IOTMS符合本文件的要求；

b) 向最高管理者报告IOTMS绩效，供其评审并作为持续改进的依据；

c) 确保在整个组织内提高对物联网安全重要性的意识；

d) 协调与IOTMS有关的内部和外部沟通（特别是与感知终端供应商、平台运营商和监管机构）。

同时，最高管理者应明确**指定一个联络点**，供相关方使用，以处理与物联网安全相关的事宜。

6. 策划

6.1 应对风险和机会的措施

6.1.1 总则

当策划IOTMS时，组织应考虑4.1中提到的事项和4.2中提到的要求，并确定需要应对的风险和机会，以：

a) 确保IOTMS可达到预期结果；

b) 预防或减少不良影响（如物联网系统被入侵、数据泄露、服务中断、合规处罚）；

c) 达到持续改进。

组织应策划：

d) 应对这些风险和机会的措施；

e) 如何将此措施整合到IOTMS过程中并予以实现及评价其有效性。

6.1.2 物联网安全风险评估

组织应定义并应用风险评估过程，以建立并维护风险准则（包括风险接受准则和评估实施准则）；识别与物联网系统相关的安全风险（如感知终端物理攻击、网络协议漏洞、平台应用漏洞、数据泄露、供应链风险、系统生存周期各阶段风险）；分析并评价风险。风险评估应特别考虑物联网系统特有的威胁和脆弱性（如资源受限设备、异构网络、物理环境暴露）。组织应保留有关风险评估过程的文件化信息。

6.1.3 物联网安全风险处置

组织应定义并应用风险处置过程，以选择适当的处置方案（通过 **ISO/IEC 27001:2022附录A** 及 **GB/T 37044-2018** 中的控制措施）。组织应**制定并维护一个《适用性声明》**，包含所选控制措施及删减的合理性说明，并制定正式的风险处置计划。组织应保留有关风险处置过程的文件化信息。

注： 组织应**建立并保持合规义务登记册**，以识别和跟踪与物联网安全相关的法律法规、标准及其他要求。

6.2 物联网安全目标及其实现的策划

组织应在相关职能和层级上建立物联网安全目标。目标应：

a) 与物联网安全方针一致；

b) 可测量（如物联网安全事件数、感知终端漏洞修复率、培训完成率、审计发现项关闭率、系统可用性指标）；
c) 考虑适用的要求；
d) 予以监视；
e) 予以沟通；
f) 视情况予以更新。
策划如何实现这些目标时，组织应确定要做什么、需要什么资源、由谁负责、何时完成、如何评价结果。

6.3 针对变更的规划

当组织确定需要对IOTMS进行变更时（如引入新的物联网设备、升级网络协议、更换平台供应商、法律法规重大变更），变更应系统地予以策划和实施。

7. 支持

7.1 资源

组织应确定并提供建立、实施、维护和持续改进IOTMS所需的资源。资源包括：具备相应能力的人员（物联网安全专家、嵌入式安全工程师等）、技术基础设施（安全芯片、加密模块、访问控制系统、日志审计系统、入侵检测系统、固件安全分析工具等）、财务资源、技术资源等。

7.2 能力

组织应：确定从事会影响组织物联网安全绩效的工作人员的必要能力（如物联网安全技术、嵌入式系统安全、网络协议安全、风险评估方法）；基于适当的教育、培训或经验确保其胜任；适用时采取措施获得必要能力（如物联网安全培训、认证），并评估有效性；保留适当的文件化信息作为能力的证据（如培训记录、认证证书）。
注：**能够访问物联网系统管理接口或敏感数据的人员应承担保密义务**。

7.3 意识

在组织控制下工作的人员应了解：
a) 物联网安全方针；
b) 其对IOTMS有效性的贡献；
c) 不符合IOTMS要求的潜在影响（尤其是对物联网系统和组织的风险）。

7.4 沟通

组织应确定与IOTMS相关的内部和外部沟通的需求，包括：沟通什么（如物联网安全策略、安全事件通知、固件更新通知）、何时沟通、与谁沟通、谁来沟通、怎么沟通。特别地，应建立与感知终端供应商、平台运营商和监管机构关于信息安全的沟通机制。

7.5 文件化信息

7.5.1 总则

组织的IOTMS应包括：本文件要求的文件化信息（如IOTMS手册、风险评估报告、风险处置

计划、适用性声明、物联网安全策略等）；组织为IOTMS有效性所确定的必要的文件化信息（如物联网系统架构图、设备清单、安全配置基线、操作流程、事件响应计划）。

7.5.2 创建和更新

创建和更新文件化信息时，组织应确保适当的标识和说明、形式、载体以及评审和批准。

7.5.3 文件化信息的控制

IOTMS及本文件所要求的文件化信息应得到控制，以确保：在需要的场合和时机可获得并适用；予以妥善保护（避免泄密、不当使用或缺失）。为控制文件化信息，适用时，组织应分发、访问、检索和使用；存储和防护；更改控制；保留和处置。

8. 运行

8.1 运行的策划和控制

组织应策划、实施和控制为满足要求和实施第6章所确定的措施所需的过程，包括建立过程准则，并按照准则实施控制。组织应控制计划内和计划外的变更，确保外部提供的过程、产品和服务受控。

8.2 物联网安全风险评估

组织应考虑6.1.2a) 所建立的准则，按计划的时间间隔或当重大变更发生时（如新物联网设备上线、网络架构变更），执行物联网安全风险评估。应保留风险评估结果的文件化信息。

8.3 物联网安全风险处置

组织应实现物联网安全风险处置计划。应保留风险处置结果的文件化信息。

8.4 物联网安全特定控制措施（依据GB/T 37044-2018）

组织应按本章节要求实施和运行特定的物联网安全控制措施，这些措施补充和细化了ISO/IEC 27001:2022附录A中的相关控制。

8.4.1 物联网安全策略（依据GB/T 37044-2018第5章）

控制

应制定和维护物联网安全策略，以管理组织的物联网安全。

实施要求：

a) 制定并维护文件化的《物联网安全策略》，该策略应由最高管理层批准。

b) 该策略应涵盖：物联网安全目标与原则；安全分区策略；系统生存周期各阶段的安全要求；基本安全防护措施（物理安全、网络安全、系统安全、应用安全、运维安全、安全管理）；合规要求。

c) 该策略应定期评审和更新（至少每年一次）。

8.4.2 安全参考模型与矩阵对照（依据GB/T 37044-2018第5章及表1）

控制

应基于物联网安全参考模型（安全分区、生存周期、基本防护措施）建立安全矩阵，明确各安全分区在生存周期各阶段所需的安全控制。

实施要求：

a) 组织应基于**GB/T 37044-2018表1“参考安全分区/生存周期”矩阵**，建立本组织的安全矩阵

对照表。

b) 安全矩阵应明确以下对应关系：

- **感控安全区**：规划设计阶段应满足5.4.1 a)~d)、5.4.2.1 a)b)、5.4.3 f)；开发建设阶段应满足5.4.1 a)~d)、5.4.2.1 a)b)、5.4.3 f)g)；运维管理阶段应满足5.4.5 a)、5.4.6 a)~d)。
- **网络安全区**：开发建设阶段应满足5.4.2.1 c)d)、5.4.2.2 a)~f)、5.4.3 a)f)g)；运维管理阶段应满足5.4.5 a)、5.4.6 a)~d)。
- **应用安全区**：规划设计阶段应满足5.4.3.1 a)~g)、5.4.3.2 a)~c)、5.4.4 a)~c)；开发建设阶段应满足5.4.3.1 a)~g)、5.4.3.2 a)~c)、5.4.4 a)~c)；运维管理阶段应满足5.4.5 a)、5.4.6 a)~d)；废弃退出阶段应满足安全存档、擦除缓存、物理销毁等要求。
- **运维安全区**：开发建设阶段应满足5.4.3.1 a)~f)、5.4.3.2 a)~c)、5.4.5 a)~c)、5.4.6 a)~d)；运维管理阶段应满足5.4.3.1 a)d)f)g)、5.4.3.2 a)~c)、5.4.5 a)~c)、5.4.6 a)~d)。

c) 安全矩阵应定期评审和更新（至少每年一次）。

8.4.3 感控安全区控制（依据GB/T 37044-2018第5.2.2条及第5.4.2条）

控制

应保护感知终端和感知控制系统的安全。

实施要求：

a) **接入安全**：各类感知终端和接入设备在接入网络时应具备唯一标识；对各类感知终端接入行为应具有身份鉴别机制；对于网络的安全接入应采取禁用闲置端口、设置访问控制策略等防护手段；对于网关、防火墙等网络边界设备，应具备安全策略配置、口令管理和访问控制等安全功能。

b) **通信安全**：物联网中的数据传输协议应有数据校验功能以确保数据传输的完整性；应采用标准化时间戳机制等技术确保数据传输的可用性；应采用技术手段对数据传输的隐私性进行保护；在网络数据交互前，应采用认证等方式为交互双方身份的可信性提供证明；应采用国家法律法规允许的加密算法对网络传输数据进行加密，确保信息的保密性；物联网系统应具备防伪基站攻击、防中间人攻击的能力。

c) **物理安全**：感知终端应具备防物理篡改、防拆卸、防环境破坏的能力。

8.4.4 网络安全区控制（依据GB/T 37044-2018第5.4.2条及第5.4.3条）

控制

应保护物联网网络基础设施的安全。

实施要求：

a) **网络隔离**：应根据安全分区实施网络隔离，不同安全区之间应有逻辑或物理隔离。

b) **访问控制**：在网络边界部署防火墙、入侵检测/防御系统，实施访问控制策略。

c) **通信加密**：对跨安全区的数据传输进行加密。

d) **系统安全**：对网络设备（路由器、交换机）进行安全配置，关闭不必要的服务，定期进行漏洞扫描和补丁管理。

8.4.5 应用安全区控制（依据GB/T 37044-2018第5.2.4条及第5.4.4条）

控制

应保护物联网应用系统的安全。

实施要求：

a) **身份认证与访问控制：**实施用户身份认证和访问权限控制，确保只有授权用户才能访问应用系统。

b) **应用安全：**对应用软件进行安全编码和测试，防止常见Web漏洞（如SQL注入、XSS）。

c) **数据安全：**对应用系统中的数据进行加密存储和传输，实施数据备份和恢复机制。

8.4.6 运维安全区控制（依据GB/T 37044-2018第5.2.5条及第5.4.5条）

控制

应保护物联网运维管控系统的安全。

实施要求：

a) **运维安全：**物联网中不同责任方应根据其职责，在物联网系统招标时，对物联网设备、系统和服务的采购部署作出规定，如规定设备、系统和服务提供方的资质要求、可信赖性等，提供系统文档的详细程度，供应链的安全要求等。

b) **人员安全：**对于物联网系统运行维护中的相关参与人员，应提出人员资质、身份审核、可信证明、诚信承诺等要求，以确保其在物联网系统维护过程中的安全可信。

c) **运维工具安全：**应对物联网系统运维的时效性、维护工具等提出安全要求，对于远程维护设备的，应对远程维护制定安全规范。

8.4.7 系统生存周期安全管理（依据GB/T 37044-2018第5.3条）

控制

应在物联网系统的全生命周期中实施安全管理。

实施要求：

a) **规划设计阶段：**在系统设计阶段应考虑安全需求，进行安全风险评估，制定安全方案。

b) **开发建设阶段：**在系统开发建设阶段应遵循安全编码规范，进行安全测试，确保系统安全上线。

c) **运维管理阶段：**在系统运维阶段应持续进行安全监控、漏洞管理、补丁更新、事件响应和定期安全审计。

d) **废弃退出阶段：**在系统废弃退出时，应安全地清除所有数据，并对设备进行安全处置。

8.4.8 物联网安全事件管理（依据GB/T 37044-2018第5.4.6条）

控制

应建立机制以管理物联网安全事件。

实施要求：

a) 建立《物联网安全事件响应程序》。

b) 在发生物联网安全事件时，应及时响应、分析和处置。

c) 应根据实际情况制定应急响应计划和配置管理策略。

d) 应对物联网系统定期开展安全评估等工作。

8.4.9 物联网第三方管理（依据GB/T 37044-2018第5.4.5条）

控制

应确保第三方（如设备供应商、平台服务商）具有足够能力保护物联网安全。

实施要求：

a) **合同约束**：与第三方签订的合同，应规定满足本组织物联网安全义务的最低技术和组织措施。

b) **供应链安全**：在招标时，对物联网设备、系统和服务的采购部署作出规定，如规定设备、系统和服务提供方的资质要求、可信赖性等，提供系统文档的详细程度，供应链的安全要求等。

c) **监控与审计**：对第三方的物联网安全活动进行监控和定期审计，确保其满足合同要求。

8.4.10 系统安全控制（依据GB/T 37044-2018第5.4.3条）

控制

应确保物联网系统的系统安全。

实施要求：

a) **防恶意代码**：应在物联网系统中的关键节点（如服务器、网关）部署防恶意代码软件，并保持更新。

b) **入侵检测与防御**：应在网络边界和关键节点部署入侵检测/防御系统，并定期更新规则库。

c) **安全配置**：应对操作系统、数据库、中间件等进行安全配置，关闭不必要的服务和端口。

d) **补丁管理**：应建立补丁管理制度，定期对系统进行漏洞扫描和补丁更新。

e) **身份鉴别**：应对系统管理员实施强身份鉴别（如多因素认证）。

8.4.11 应用安全控制（依据GB/T 37044-2018第5.4.4条）

控制

应确保物联网应用系统的安全。

实施要求：

a) **应用安全开发**：应在应用开发过程中遵循安全编码规范，进行安全测试（包括静态代码分析和动态安全测试）。

b) **Web应用安全**：应防范常见Web应用攻击（如SQL注入、跨站脚本攻击、跨站请求伪造等）。

c) **身份认证与访问控制**：应对应用用户实施身份认证和基于角色的访问控制。

d) **会话管理**：应对用户会话进行安全管理，包括会话超时、会话锁定等。

e) **输入验证**：应对用户输入进行验证和过滤，防止注入攻击。

8.4.12 数据安全控制（依据GB/T 37044-2018第5.4.3条）

控制

应确保物联网系统中数据的保密性、完整性和可用性。

实施要求：

a) **数据完整性**：物联网中的数据传输协议应有数据校验功能以确保数据传输的完整性。

b) **数据可用性**：应采用标准化时间戳机制等技术确保数据传输的可用性。

c) **数据隐私性**：应采用技术手段对数据传输的隐私性进行保护。

d) **数据保密性**：应采用国家法律法规允许的加密算法对网络传输数据和存储数据进行加密。

e) **数据备份**：应定期对系统中的关键数据进行备份，并进行恢复测试。

8.4.13 安全审计控制（依据GB/T 37044-2018第5.4.4条）

控制

应对物联网系统中的重要安全事件进行审计。

实施要求：

a) **审计范围**：应对用户登录、权限变更、敏感数据访问、系统配置变更、安全事件等关键活动进行审计。

b) **审计记录**：审计记录应包括事件时间、用户身份、事件类型、事件结果等信息。

c) **审计日志保护**：应保护审计日志的完整性和保密性，防止非授权修改或删除。

d) **审计日志审查**：应定期审查审计日志，识别潜在的安全威胁和异常行为。

9. 绩效评价

9.1 监视、测量、分析和评价

组织应确定：需要被监视和测量的内容（包括物联网安全过程绩效、安全事件、设备漏洞修复率、培训完成率、合规性偏差等）；适用的方法；何时执行；谁应执行；何时分析和评价结果。组织应评价物联网安全绩效以及IOTMS的有效性。**确保用于监视与测量的资源（如安全监控平台、日志分析系统）的准确性**。

9.1.2 合规性评价

组织应建立、实施并保持程序，以定期评价其对适用法律法规（特别是物联网安全相关法律）、标准及自身IOTMS要求的遵守情况。**合规性评价应至少每年进行一次**，并**保留合规性评价报告作为成文信息**。

9.2 内部审核

组织应按策划的时间间隔进行内部审核，以提供有关IOTMS符合性及有效性的信息。审核员应确保客观性和公正性。审核结果应报告给相关管理层。

9.3 管理评审

最高管理者应按计划的时间间隔评审IOTMS，以确保其持续的适宜性、充分性和有效性。管理评审应考虑：

a) 以往管理评审措施的状态；

b) 内外部的变化（如新的物联网安全法规、物联网技术发展、设备供应商变更）；

c) 绩效信息（包括：物联网安全事件趋势、设备漏洞修复率、**外部供方（如设备供应商、平台服务商）的绩效**、合规性偏差、风险评估与处置状态、改进机会等）；

d) 持续改进的机会。

评审输出应包括与持续改进机会及IOTMS变更需求相关的决定。

10. 改进

10.1 持续改进

组织应持续改进IOTMS的适宜性、充分性和有效性。

10.2 不符合与纠正措施

当发生不符合时，组织应：做出应对、控制并纠正，处置后果；评价是否需要采取措施消除原因；实施所需的措施并评审有效性；必要时对IOTMS进行更改。应保留文件化信息作为不符合性质及后续采取措施的证据。**推荐预防措施**以防范潜在不符合的发生（例如，通过定期物联网安全评估，预防新设备或新协议带来的安全风险）。

————————————