

SZCES

深圳市建设工程标准学会标准

T/SZCES XX – 2025

建筑隐私安全性评价标准

Evaluation standards for building privacy and security

（征求意见稿）

2025-XX-XX 发布

2025-XX-XX 实施

深圳市建设工程标准学会标准

建筑隐私安全性评价标准

Evaluation standards for building privacy and security

T/SZCES XX - 2025

2025 深 圳

目 次

1	总 则	1
2	术 语	2
3	基 本 规 定	3
4	民用建筑智能化系统中个人信息的判定	5
5	智能化子系统中个人信息的要求	7
5.1	信息设施系统	7
5.2	建筑设备管理系统	7
5.3	公共安全系统	8
5.4	其他综合及集成系统	9
	本标准用词说明	11
	引用标准名录	12

Content

1	General Provision	1
2	Terms	2
3	Basic Provisions	3
4	Determination of personal information in intelligent system of civil building	5
5	Protection requirements of personal information in intelligent subsystem	7
5.1	Information facility system	7
5.2	Construction equipment management system	7
5.3	Public safety system	8
5.4	Other integrated and integrated systems	9
	This standard term description	11
	Reference standard list	12

前 言

根据深圳市建设工程标准学会团体标准编制计划和要求，标准编制组经广泛调查研究，认真总结实践经验，参考有关国内外先进标准，结合深圳市的实际，并在广泛征求意见的基础上，编制了本标准。

本标准主要技术内容是：1.总则；2.术语；3.基本规定；4.民用建筑智能化系统中个人信息的判定；5.智能化子系统中个人信息的保护要求。

本标准由深圳市住房和建设局提出并归口管理，由深圳市建筑科学研究院股份有限公司负责具体技术内容的解释。本标准实施过程中如有意见或建议，请寄送湾区（深圳）绿色技术有限公司（地址：深圳市福田区梅坳三路 29 号建科大楼，邮编：518049），以供今后修订时参考。

本标准主编单位：深圳市建筑科学研究院股份有限公司

本标准参编单位：上海数据交易所、公安部第三研究所、湾区（深圳）绿色技术有限公司、北京星河卓越科技有限公司、深圳市绿米联创科技有限公司

本标准主要起草人员：谢泽伟 王润垠 任鹏飞 王庆 余刚 刘超

本标准主要审查人员：

本标准主要指导人员：

1 总 则

1.0.1 为全面落实《中华人民共和国个人信息保护法》相关要求，在推进建筑行业数字化、智能化的同时，规范民用建筑智能化系统（下称“智能化系统”）的个人信息处理行为，制定本标准。

1.0.2 本标准适用于民用建筑智能化系统涉及个人信息的保护。

1.0.3 民用建筑智能化系统的个人信息保护要求除应符合本标准外，尚应符合国家和地方现行有关标准的规定。

2 术 语

2.0.1 个人信息 (personal information)

个人信息是以电子或者其他方式记录的与已识别或者可识别的自然人有关的各种信息，不包括已进行匿名化处理的信息。

2.0.2 匿名化 (anonymization)

匿名化是指个人信息经过处理后无法识别特定自然人且不能复原的一种过程。

2.0.3 密态关联 (anonymous state intersection)

是指两个以上的数据集在无法识别数据描述对象的状态下，加工有共同属性数据内容的过程。

2.0.4 智能化子系统 (intelligent subsystem)

本标准所指的智能化子系统包括信息设施系统、建筑设备管理系统、公共安全系统、信息化应用系统和智能化集成系统。

2.0.5 边缘计算 (edge computing)

边缘计算是指在靠近感知设备或数据源头的网络边缘侧，融合网络、计算、存储、应用等核心能力，就近提供边缘智能服务的一种分布式计算模式。

3 基本规定

3.1 应明确智能化系统个人信息保护的责任主体，因管理或服务职责直接持有或管理数据资源的机构有责任保护数据中所包含的个人信息。

3.2 智能化系统涉及个人信息保护分为以下三种不同目的：

- 1 以防止无关方不当获取个人信息为目的；
- 2 以证明己方有资格处理个人信息为目的；
- 3 以控制相关方超范围处理个人信息为目的。

3.3 当需要防止无关方不当获取个人信息时，涉及个人信息的系统应当达到网络安全等级保护二级的要求。

3.4 当需要处理己方有资格处理个人信息时：

- 1 如涉及个人信息数据处理，应实施告知并取得个人同意；
- 2 如需对个人信息执行匿名化处理时，参照《信息安全技术 个人信息去标识化指南》GB/T 37964-2019、《信息安全技术 个人信息安全规范》GB/T 35273-2020的指引实施处理。

3.5 当需要控制相关方超范围处理个人信息时，在涉及多方数据跨域处理过程中，提供方和接收方两方应当分别区分自身数据处理行为是否涉及个人信息，实施差异化的告知同意。

1 若选择向他方提供的路径，提供方宜实施增强告知并取得单独同意，接收方无需实施告知同意。但接收者处理活动超出提供者实施的告知同意范围时，接收方需重新实施一般告知并取得明示同意；

2 若选择委托处理的路径，提供方宜实施一般告知并取得明示同意，接收方无需实施告知同意。但接收者处理活动超出委托合同约定范围，或超出提供方实施的告知同意范围时，双方需重新选择处理路径并实施；

3 若选择匿名化处理的路径，提供方与接收方均无需实施告知同意；

4 若选择密态关联的路径，提供方与接收方均无需实施告知同意。但接收方处

理活动超出自身活动已有的告知同意范围时，接收者需重新实施一般告知并取得明示同意。

3.6 个人信息的存储周期分为短期、中期和长期。其中，短期存储原则上不超过 3 天，中期存储原则上不超过 90 天。

4 民用建筑智能化系统中个人信息的判定

4.1 民用建筑智能化系统中个人信息的分类与判定应符合表 4.1。

表 4.1 智能化系统中个人信息的分类与判定

智能建筑系统类型			个人信息类型	个人信息列举
智能化集成系统		信息设施系统	个人设备信息	指包括硬件序列号、设备 MAC 地址、软件列表、唯一设备识别码（如 IMEI/AndroidID/IDFA/OpenUDID/GUID/SIM 卡 IMSI 信息等）等在内的描述个人常用设备基本情况的信息
			网络身份标识信息	个人信息主体账号、IP 地址、个人数字证书等
			个人通信信息	通信记录和内容、短信、彩信、电子邮件，以及描述个人通信的数据（通常称为元数据）等
	信息化应用系统		个人上网记录	指通过日志储存的个人信息主体操作记录，包括网站浏览记录、软件使用记录、点击记录、收藏列表等
			个人基本资料	个人姓名、生日、性别、民族、国籍、个人电话号码、电子邮件地址等
		公共安全系统	个人身份信息	身份证、军官证、护照、工作证、出入证等
			个人生物识别信息	指纹、声纹、掌纹、耳廓、虹膜、面部识别、步态、动作特征等
			个人位置信息	包括建筑内行踪轨迹、精准定位信息、住宿信息等
			个人影像信息	内容关于个人的照片、视频信息等
		建筑设备管理系统	个人设备使用习惯	空调温度设定偏好、照明开关时间、电梯使用频次、智能窗帘开合习惯、智能家电操作记录（如洗衣机模式选择）等
			个人能源使用信息	分时用电记录（如每日用电时段）、用水量统计、燃气消耗数据、太阳能使用效率（与用户行为关联的能源数

智能建筑系统类型			个人信息类型	个人信息列举
				据)等
			个人行为信息	设备异常操作记录(如非授权访问尝试)、节能模式选择偏好、设备故障报修记录(含用户联系方式)等

4.2 民用建筑智能化系统中敏感个人信息的分类与判定应符合表 4.2。

表 4.2 智能化系统中敏感个人信息的分类与判定

个人生物识别信息	指纹、声纹、掌纹、耳廓、虹膜、面部识别、步态、动作特征等
个人身份信息	身份证、军官证、护照、工作证、出入证等
其他信息	通信记录和内容、通讯录、好友列表、群组列表、行踪轨迹、网页浏览记录、住宿信息、精准定位信息等

5 智能化子系统中个人信息的要求

5.1 信息设施系统

5.1.1 信息接入系统应符合《有线接入网设备安装工程设计规范》YD/T 5139-2019的要求。系统应仅记录为确保安全接入所必需的用户身份信息。

5.1.2 信息接入系统应仅用于提供网络接入服务，不应超出该用途范围使用，也不应委托未取得电信业务经营许可的第三方进行运营。

5.1.3 移动通信室内信息覆盖系统在非必要情况下不得收集IMEI等个人设备标识符。确因优化信号覆盖需要而必须收集时，应设定短期的存储期限。

5.1.4 用户电话交换系统的通话记录等信息应设定短期存储期限。如需长期保存，应对相关数据进行加密处理并设置访问权限。

5.1.5 信息网络系统应遵循个人信息最小必要存储原则，并应对IP地址信息进行加密存储。

5.1.6 公共广播系统、信息导引及发布系统应建立内容发布审核机制，以保护其中可能涉及的个人信息。

5.1.7 会议系统应在会议结束后自动清除所有参会人员的个人信息，并且不应将其上传至任何其他信息系统。

5.2 建筑设备管理系统

5.2.1 建筑设备监控系统在设备维修时应选择具备相应资质的服务商；设备运行参数不应传输至本建筑智能化系统之外。

5.2.2 建筑能效监管系统收集的个人用户习惯等数据不应传输至本建筑智能化系统之外。公共建筑能效监管系统中的数据不应传输给未经政府授权的运营方。

5.2.3 智能家居设备应在征得用户同意的前提下遵循最小必要原则收集个人信息。个人信息处理者不得因个人未同意或已撤回同意而拒绝提供产品或服务，但当处理

个人信息是提供产品或服务所必需时，不在此限。

5.3 公共安全系统

5.3.1 入侵报警系统在警报触发时记录的时间、地点信息，以及其中包含人脸识别特征等生物识别信息的相关记录，应采用加密方式存储并限制访问权限；不应将上述信息传输至本建筑智能化系统之外。

5.3.2 视频安防监控系统在公共场所进行视频、音频或图像监控时，应符合以下要求：

1 公共场所安装安防监控摄像头时，应在显著位置设置醒目的提示标识，以告知公众该区域正处于监控之中；

2 在私人场所的出入口自行安装摄像头时，应事先征得该过道内其他相关方的同意；

3 包含个人信息的视频、音频或图像数据应采用中期存储方式，并进行加密处理，设置访问权限，不应传输至本建筑智能化系统之外；

4 民用建筑公共场所安装视频、音频或图像采集设备时，应当确保此举确属维护公共安全所必需，并遵守国家有关规定，同时设置显著的提示标识。所收集的个人信息应依据相关法律法规进行处理。

5.3.3 出入口控制系统应符合以下个人信息保护要求：

1 用于出入口控制的个人信息收集应符合《信息安全技术 个人信息安全规范》GB/T 35273-2020 第 5.4 条的要求；

2 出入口控制系统应保留非生物识别信息的身份验证和通行授权方式；

3 出入口控制系统中涉及个人信息的视频、音频或图像数据应符合本标准 5.3.2 的要求；

4 采集的生物识别信息应仅用于出入口控制，未经个人同意或未进行匿名化处理，不应将其传输至本建筑智能化系统之外的其他系统或平台；

生物识别信息的存储宜采用边缘计算方式处理，以避免服务器留存原始数据。

5.3.4 智能卡应用系统如涉及持卡人个人信息，应符合以下要求：

- 1 不应强制采集持卡人的生物识别信息；
- 2 持卡人个人信息应仅用于智能卡相关的应用功能；
- 3 持卡人个人信息应加密存储，并设置访问权限；
- 4 未经个人同意或未进行匿名化处理，不应将持卡人的个人信息传输至本建筑智能化系统之外的其他系统或平台。

5.3.5 访客系统如涉及访客身份信息，应符合以下要求：

- 1 不宜强制收集访客的身份证件号码等身份信息；
- 2 不应强制采集访客的人脸识别特征等生物识别信息；
- 3 访客身份信息应采用短期、加密存储方式，并设置访问权限；
- 4 未经个人同意或未进行匿名化处理，不应将访客身份信息传输至本建筑智能化系统之外的其他系统或平台。

5.3.6 停车管理系统涉及车牌号码、入场时间等信息时，应符合以下要求：

- 1 车牌号码、入场时间等信息应仅用于停车出入授权及缴费功能；
- 2 不应强制采集人脸识别特征等生物识别信息；
- 3 采集视频或图像信息的停车管理系统应符合本标准 5.3.2 的要求；
- 4 车牌号码、入场时间等信息应采用短期、加密存储方式，并设置访问权限；
- 5 如车牌号码、入场时间等信息属于个人信息，则未经个人同意或未进行匿名化处理，不应将其传输至本建筑智能化系统之外的其他系统或平台。

5.4 其他综合及集成系统

5.4.1 安全防范综合管理平台、公共服务系统、物业管理系统，以及由它们组合或集成的其他信息化应用系统或智能化集成系统，如涉及个人信息，应符合以下要求：

- 1 未经个人同意或未进行匿名化处理，不应收集个人信息；
- 2 所收集的个人信息应加密存储，并设置访问权限；
- 3 未经个人同意或未进行匿名化处理，不应将个人信息传输至本建筑智能化系

统之外的其他系统或平台。

本标准用词说明

1 为了便于在执行本标准条文时区别对待,对要求严格程度不同的用词说明如下:

1) 表示很严格,非这样做不可的用词:

正面词采用“必须”,反面词采用“严禁”;

2) 表示严格,在正常情况下均应这样做的用词:

正面词采用“应”,反面词采用“不应”或“不得”;

3) 表示允许稍有选择,在条件许可时首先应这样做的用词:

正面词采用“宜”,反面词采用“不宜”;

4) 表示有选择,在一定条件下可以这样做的用词,采用“可”。

2 条文中指明应按其他有关的标准、规范执行的写法为“符合……的规定”或“应按……执行”;非必须按所指定的标准和规范执行的写法为“可参照……执行”。

引用标准名录

- 1 《智能建筑设计标准》 GB50314-20152
- 2 《信息安全技术 个人信息安全规范》 GB/T35273-2020
- 3 《信息安全技术 网络安全等级保护基本要求》 GB/T 22239-2019
- 4 《信息安全技术 个人信息处理中告知和同意的实施指南》 GB/T-42574-2023
- 5 《信息安全技术 个人信息去标识化指南》 GB/T 37964-2019
- 6 《有线接入网设备安装工程设计规范》 YD/T 5139-2019