

合肥市公安局 合肥市住房保障和房产管理局 文件

合公办〔2021〕38号

关于印发《智慧平安小区运维管理实施办法》 的通知

各县（市）区公安局、物业管理部门：

为加强我市智慧平安小区运维管理工作，确保智慧平安小区正常运行，更好服务平安合肥建设，根据《合肥市住宅小区安全防范设施建设和管理实施办法》（合政办〔2019〕21号）要求，结合工作实际，市公安局、市住房保障和房产管理局联合制定《智慧平安小区运维管理实施办法》，现将本办法印发给你们，请认真组织实施。

合肥市公安局

合肥市住房保障和房产管理局

2021年2月3日

合肥市智慧平安小区运维管理实施办法

一、总 则

第一条 为加强住宅小区管理，提升服务管理水平，不断增强广大居民的幸福感、获得感和安全感，制定本办法。

第二条 本办法适用于全市建成投入使用的智慧平安小区运维管理工作。

第三条 运维管理工作按照“谁使用、谁维护、谁管理、谁负责”的原则，“政府主导、企业参与、属地管理、因地制宜”的原则。商业住宅小区安防设施的使用维护，应当由建设单位或者产权人依照物业管理的规定选聘物业服务企业，实施统一使用维护。政府服务管理小区安防设施的使用维护，应当由街道、社区依照物业管理的规定选聘物业服务企业或者按照相关规定实施统一使用维护。

第四条 智慧平安小区运维管理要落实专人保管，定期维护，保证数据安全，确保运行稳定可靠。

二、职责分工

第五条 市公安局负责智慧平安小区运维平台建设，定期抽查并通报全市智慧平安小区运行管理及小区可防性案件发案情况；各分县市、开发区公安分局要参照市局工作职责，细化本单

位工作任务，调度辖区派出所监督指导物业服务企业做好智慧平安小区运维管理工作，加强对物业服务企业的业务培训，规范物业服务企业开展的安全防范管理工作，对恶意破坏智慧平安小区正常运行的行为，要坚决打击处理；社区民警对辖区智慧平安小区每月不少于1次检查指导，协调建设单位、物业企业和运维单位在小区日常运维工作中及时排除故障、解决问题，确保智慧平安小区正常运行。

第六条 市住房保障和房产管理局负责督促各物业管理部门和物业服务企业做好配合和支持工作，将智慧平安小区管理运维情况纳入年度目标考核和物业服务项目考核；各区县（市）区、开发区住建部门将智慧平安小区运维管理纳入到日常检查内容中，发现问题及时通报整改。

第七条 物业服务企业负责小区安防设施日常管理，配合公安机关做好信息采集工作，物业服务企业应当按照《保安服务管理条例》、《公安机关实施保安服务管理条例办法》等法律法规的要求，自行招用或从保安公司聘用具有从业资格的保安员负责安防设施管理应用，每天对小区安防设施进行巡检，严禁私自将安防设施断电、断网、停机等，不得将建设好的车闸、道闸随意敞开，做好外来人员、车辆出入登记工作，发现故障及时通报建设公司进行维护，定期组织学习《智慧平安小区信息网络安全管理制度》（附件），坚决避免数据被故意、过失或以其他渠道泄漏。

三、考核奖惩

第八条 对因智慧平安小区运维管理不力影响小区平安建设和群众安全感的物业服务企业，公安机关要督促其整改，对照《保安服务管理条例》进行检查，发现问题通报仍未整改的，应进行相应处罚；对泄露和违规使用居民个人信息的责任人和单位负责人按照相关法律进行处罚；市住房保障和房产局将智慧平安小区运维管理纳入物业服务项目创优考核指标体系，对被公安机关处罚的项目实行“一票否决制”。

第九条 对管理运维及小区平安建设成绩突出的，各区县市公安机关联合住建部门开展平安小区评定授牌，对获得表彰的小区物业服务企业，适当给予经费激励补助。

附件

智慧平安小区信息网络安全管理制度

智慧平安小区物业服务企业或实际承担小区物业管理职能的单位应落实以下安全管理制度：

一、人员安全管理

(1) 应成立网络安全工作组织，负责人由单位主要负责人担任。

(2) 应制定符合实际工作需要的网络安全管理制度，必要时应根据监管要求进行评审、更新。

(3) 应对系统操作员等关键岗位人员进行网络安全意识和操作技能培训，并进行必要的考核。

(4) 应与智慧平安小区系统相关的管理、运维以及其他关键岗位人员签订保密协议或保密承诺书，不可泄露用户的敏感信息。

(5) 应做好人员管理工作，尤其是离岗时应签署离岗保密协议和承诺书，收回如钥匙、USBkey、帐户等与智慧平安小区系统相关的资产。

二、计算机安全管理

(1) 物业管理电脑应处于防风、防雨的室内。

(2) 物业管理电脑所在房间应通过门禁等方式进行有效控

制。

(3) 物业管理电脑应设置屏保及密码，自动锁屏时间不超过 5 分钟。

(4) 物业管理电脑应禁用访客帐户，修改默认帐户口令，并设置满足复杂度要求的口令（口令长度不少于 8 位，由大、小写字母、数字和特殊字符的组成）。

(5) 物业管理电脑应安装杀毒软件，定期查杀并保持病毒库更新。

(6) 物业管理电脑登入后台管理系统，浏览器不应设置保存密码。

(7) 物业管理电脑不应安装不可信任的软件，操作员应定期检查操作系统版本，及时在线更新。

(8) 应做好移动介质、文档管理工作，移动介质插入电脑运行前做好病毒检测工作。

(9) 物业管理电脑与办公电脑应专机专用，避免混用造成攻击、病毒传播等安全隐患。

(10) 来路不明的电子邮件及附件不得随意打开，附件在使用前应进行病毒检查，确保无病毒后才能使用。

三、个人信息保护制度

(1) 不得违反法律、行政法规的规定和双方的约定收集、使用个人信息，并应当依照法律、行政法规的规定和与用户的约定，处理保存个人信息。

(2) 收集、使用个人信息，应当遵循合法、正当、必要的原则，公开收集、使用规则，明示收集、使用信息的目的、方式和范围，并经被收集者同意。

(3) 不得收集与提供的服务无关的个人信息。

(4) 不得泄露、篡改、损毁收集的个人信息；未经被收集者同意，不得向他人提供个人信息。

(5) 在发生或者可能发生个人信息泄露、毁损、丢失的情况时，应当立即采取补救措施，按照规定及时告知用户并向有关主管部门报告。

(6) 小区数据采集应仅采集与业务相关的数据，避免出现未授权采集、超范围采集的情况。

(7) 小区数据采集及管理终端不应保存敏感个人信息，如身份证号、生物特征、财产信息等。

(8) 应禁止未授权访问或非法使用用户个人信息。

四、相关法律法规

(1) 《刑法》第二百五十三条之一 违反国家有关规定，向他人出售或者提供公民个人信息，情节严重的，处三年以下有期徒刑或者拘役，并处或者单处罚金；情节特别严重的，处三年以上七年以下有期徒刑，并处罚金。

(2) 《网络安全法》第五十九条 网络运营者不履行本法第二十一条、第二十五条规定的网络安全保护义务的，由有关主管部门责令改正，给予警告；拒不改正或者导致危害网络安全等后

果的，处一万元以上十万元以下罚款，对直接负责的主管人员处五千元以上五万元以下罚款。

(3)《网络安全法》第六十四条 网络运营者、网络产品或者服务的提供者违反本法第二十二条第三款、第四十一条至第四十三条规定，侵害个人信息依法得到保护的权利的，由有关主管部门责令改正，可以根据情节单处或者并处警告、没收违法所得、处违法所得一倍以上十倍以下罚款，没有违法所得的，处一百万元以下罚款，对直接负责的主管人员和其他直接责任人员处一万元以上十万元以下罚款；情节严重的，并可以责令暂停相关业务、停业整顿、关闭网站、吊销相关业务许可证或者吊销营业执照。