能源管理系统使用和维护的管理制度

一、总则

为确保能源管理系统稳定、高效运行，充分发挥其在建筑能源监测、分析与控制中的作用，特制定本管理制度。

本制度适用于黑岩村各类使用能源管理系统的建筑，包括村民住宅、民宿及公共建筑等。相关人员应严格遵守本制度，保障能源管理系统的正常使用与维护。

二、使用管理制度

人员权限管理

设立系统管理员、普通用户等不同权限角色。系统管理员负责系统的整体配置、用户权限管理、数据备份等高级操作；普通用户仅具备能源数据查询、简单报表查看等基本权限。用户账号采用实名注册，严格保密账号密码，不得转借他人使用。如发现账号异常登录，应立即通知系统管理员。

日常使用规范

操作人员在使用能源管理系统前，应接受系统操作培训，熟悉系统界面、功能及操作流程。

按照规定的操作流程进行数据查询、报表生成、设备控制等操作。严禁随意更改系统参数、删除系统数据。

定期对系统进行登录检查，确保系统运行正常。如发现系统故障或数据异常，应及时记录并报告给相关维护人员。

数据使用规定

能源数据属于重要信息，仅用于建筑能源管理分析、节能决策制定等相关工作，未经授权不得对外泄露。

如需使用系统中的历史能源数据进行研究、报告撰写等工作，需提前向系统管理员申请，经批准后方可使用。使用过程中应遵循数据使用规范，不得篡改数据。

三、维护管理制度

日常维护

维护人员每日对能源管理系统进行巡检，检查系统硬件设备（如数据采集器、服务器等）是否正常运行，网络连接是否稳定。

清理系统设备表面灰尘，确保设备散热良好。检查数据采集传感器是否有损坏、移位等情况，如有问题及时修复或更换。

定期对系统软件进行更新，安装最新的补丁程序，确保系统安全性和稳定性。

定期维护

每周对系统数据进行备份，将备份数据存储在外部存储设备中，并定期对备份数据进行检查，确保数据可恢复。

每月对系统进行性能检测，包括数据传输速率、系统响应时间等指标。如发现性能下降，及时进行优化调整。

每季度对能源管理系统进行全面维护，包括硬件设备的深度保养、软件系统的全面检查与修复等。

故障处理

当能源管理系统出现故障时，维护人员应立即响应，按照故障处理流程进行排查和修复。如遇重大故障，应及时报告给相关负责人，并通知受影响的用户。

建立故障记录档案，详细记录故障发生时间、故障现象、故障原因、处理措施及处理结果等信息。定期对故障记录进行分析，总结故障发生规律，采取预防措施，降低故障发生率。

四、异常情况应急处理措施

数据异常处理

数据缺失：若发现某时间段内能源数据缺失，维护人员应首先检查数据采集设备是否正常运行，查看设备日志，确定是否因设备故障导致数据未采集。若设备正常，检查数据传输链路是否存在中断或丢包情况。对于因设备故障导致的数据缺失，及时修复设备，并从备份数据中尝试恢复缺失数据；若因传输问题，排查网络故障点，修复后重新获取缺失数据。同时，在运行记录中详细记录数据缺失时间、原因及处理情况。

数据错误：当发现采集的能源数据明显错误，如电力数据出现负值或远超正常范围，维护人员应立即核实传感器是否损坏、校准参数是否正确。若传感器损坏，及时更换传感器，并对更换前的错误数据进行标记和修正。若校准参数问题，重新校准传感器，并对受影响的数据进行修正。对于已发布的报表或分析结果中涉及错误数据的部分，及时通知相关用户，并重新生成正确的报表和分析。

设备故障处理

数据采集器故障：若数据采集器出现死机、无法启动等故障，维护人员应先尝试重启设备。若重启后仍无法正常工作，检查设备电源连接、硬件线路是否松动或损坏。对于硬件损坏的情况，及时更换故障部件，并重新配置采集器参数，确保其正常采集数据。在故障处理期间，若有备用数据采集器，应及时启用备用设备，保证能源数据采集的连续性。

服务器故障：当服务器出现故障，如系统崩溃、无法访问等，系统管理员应立即启动应急预案。首先，检查服务器日志，确定故障原因，如软件错误、硬件故障等。对于软件错误，尝试进行系统修复或还原操作；若为硬件故障，及时联系硬件供应商进行维修或更换。在服务器恢复正常前，若有异地备份服务器，切换至备份服务器运行，确保能源管理系统的基本功能可用。同时，通知所有用户服务器故障情况及预计恢复时间。

网络中断处理

局域网中断：若能源管理系统所在局域网出现中断，维护人员应立即排查网络设备（如交换机、路由器）是否正常工作，检查网络线路是否有破损、松动等情况。对于网络设备故障，及时更换或修复故障设备；对于线路问题，修复或更换线路。在网络中断期间，若有备用网络链路（如 4G/5G 网络备用方案），及时切换至备用链路，保障数据传输。同时，在运行记录中记录网络中断时间、原因及恢复时间。

互联网中断（若系统涉及远程数据传输或云服务）：若互联网连接中断，影响系统与远程服务器或云平台的数据交互，维护人员应联系网络服务提供商，确认是否为外部网络故障。若为外部故障，等待网络服务提供商修复，并及时向用户通报情况。若为内部网络设置或设备问题，排查防火墙、路由器等设备的设置，修复故障。在互联网中断期间，若本地存储有足够的历史数据，可继续提供本地数据的查询和分析服务。

安全漏洞与攻击处理

安全漏洞发现：若系统检测到存在安全漏洞，系统管理员应立即评估漏洞的风险等级。对于高风险漏洞，及时采取临时防护措施，如关闭相关端口、限制访问等。同时，联系系统供应商获取漏洞修复补丁，在测试环境中验证补丁的有效性后，尽快在生产环境中安装补丁，修复漏洞。在修复完成后，对系统进行全面安全检测，确保漏洞已完全修复。

网络攻击：当能源管理系统遭受网络攻击，如恶意软件入侵、DDoS 攻击等，系统管理员应立即启动应急响应机制。首先，切断受攻击设备与网络的连接，防止攻击扩散。分析攻击来源和方式，收集相关证据。对于恶意软件入侵，使用专业的杀毒软件进行查杀，并对受感染的数据和系统进行修复和恢复；对于 DDoS 攻击，联系网络服务提供商进行流量清洗，恢复网络正常运行。同时，加强系统安全防护措施，如更新防火墙规则、强化用户认证机制等，防止再次遭受攻击，并将攻击情况及时报告给相关安全部门。