

客户安全概览

本文面向客户 IT、OT、安全和设施团队，说明 ClimaMind 在生产部署中的安全边界、部署控制和客户数据保护措施。

ClimaMind 面向客户楼宇环境采用清晰的部署边界、受控的边缘到云端通信、客户批准的 BMS 连接，以及可审计的运行记录。本 PDF 是审查材料，不是认证声明。

部署架构

客户用户、ClimaMind 云服务、站点数据、边缘设备和客户 BMS 通过明确生产路径保持分离。

- 客户用户通过 TLS 访问 dashboard。
- Secure Cloud Gateway 验证边缘通信和批准后的更新。
- 站点数据存储存储在 ClimaMind 云服务中，并与客户 BMS 控制路径分离。
- 边缘设备出站连接 ClimaMind 服务；客户 BMS 保留在客户现场边界内。

数据分级与处理方式

分级	示例	静态加密	传输加密	处理方式
Public	公开网站内容和已发布文档	否	否	批准后可对外分发。
Internal	非公开运行笔记和实施细节	否	是	限 ClimaMind 人员和批准的协作者。
Confidential	站点元数据、遥测、dashboard、诊断和配置	是	是	访问受控；仅用于交付、支持、运行和批准后的分析。
Restricted	凭证、密钥、设备身份、BMS 访问和写入授权	是	是	存放在 AWS Secrets Manager；访问严格受限。

数据保护

部署安全聚焦站点数据、dashboard 访问、运行配置和边缘遥测。

- 公开网站和已发布安全概览材料属于公开信息。
- 非公开运行笔记和实施细节属于内部信息。
- 客户站点元数据、楼宇遥测、dashboard 数据、诊断、支持上下文和客户配置属于机密信息。
- 凭证、证书、API token 和签名材料属于受限密钥，存放在 AWS Secrets Manager。
- 生产访问基于角色，并限制在运行需要内。

边缘设备安全

边缘设备使用出站、认证的云端通信和窄范围更新路径。

- 边缘设备只向批准的 ClimaMind 云端点发起出站通信。
- TLS 和证书验证保护云端通信。
- 遥测上传使用认证和签名通信。
- 更新下发有版本记录，使用认证路径，并保留回退。
- 本地运行配置将服务限制在客户现场部署所需职责内。

Building Control Safety

BMS 连接限制在客户批准的路径和点位内，控制行为有边界。

- 连接限制在客户批准的 BMS 端点和点位映射内。
- 先读后控的部署方式支持控制前验证。
- BMS 写入采用 allowlist，并限制在批准点位。
- 控制动作保留本地 BMS 权限、操作员流程和客户定义的运行约束。
- 回退和 fail-safe 行为保留既有楼宇运行方式。

远程支持访问

远程支持需要明确批准、限定时间，并符合客户现场策略。

- 正常部署不要求常开的远程管理隧道。
- 部署不要求默认常开的 VPN、SSH 或 RDP 路径。
- 支持访问可根据客户策略使用固定源 IP、证书验证或现场访问。
- 支持会话按任务和时间窗口批准，并作为安全相关事件记录。

审计记录

安全相关事件记录在 ClimaMind 云系统中；如部署要求，也可保存到客户指定证据位置。

- Dashboard 认证与管理访问。
- 部署配置变更，以及模型或配置更新。
- 遥测上传状态、更新下发事件和边缘到云认证事件。
- BMS 写入尝试、批准的控制动作和远程支持会话。

本概览用于供应商审查、安全 intake 和部署规划，不暴露内部实施流程。