Customer Security Overview

This document summarizes ClimaMind's security boundary, deployment controls, and customer data protection measures for customer-impacting production systems.

ClimaMind's security program focuses on access control, production change control, data protection, edge device identity, secure telemetry ingestion, building control safeguards, incident response, vendor risk, and evidence retention.

System Boundary

ClimaMind maintains a defined boundary around the customer data and customer environments used by its production deployments.

Customer-impacting areas include:

- customer data storage and access;
- customer dashboards and data access controls;
- edge devices deployed for customer sites;
- secure telemetry ingestion from edge devices;
- credentials, secrets, and device identity provisioning;
- building control paths where ClimaMind reads from or writes to BAS systems.

```
flowchart LR
  User["Customer Users"]
  Dashboard["ClimaMind Dashboard"]

  subgraph Cloud["ClimaMind Cloud"]
    Gateway["Secure Cloud Gateway"]
    SiteData["Site Data"]
    Internal["ClimaMind Internal Services"]
  end

  subgraph Site["Customer Site"]
    Edge["ClimaMind Edge Device"]
    BAS["Customer BAS<br/>Approved Endpoint / Gateway"]
  end

  User -- "TLS" --> Dashboard
  Dashboard -- "TLS" --> Gateway
  Internal --> Gateway
  Edge -- "Telemetry upload<br/>TLS + certificate validation<br/>authenticated / signed" --> Gateway
  Gateway --> SiteData
  Gateway -- "Versioned model/config update<br/>rollback path" --> Edge
  Edge -- "Read + allowlisted writes<br/>customer-approved connectivity" --> BAS
```

Customer Data

ClimaMind production deployments may process:

- customer site and device metadata;
- building telemetry such as temperatures, pressures, power, and BAS registers;
- control decisions, requested control actions, model or controller versions, and write results;

- operational diagnostics needed to support the deployment.

Personal information used for CRM, sales, or customer communication is handled outside the edge deployment boundary. It is not part of the edge device or building control runtime.

Production application and edge-to-cloud communications use encrypted transport such as TLS. Confidential customer data uses managed encryption at rest, and restricted credentials and secrets are stored in AWS Secrets Manager.

ClimaMind classifies deployment data as follows:

Classification	Examples	Handling
Public	Public website content, published marketing materials, public documentation	Approved for external distribution.
Internal	Non-public operational notes, implementation details, non-customer internal planning	Limited to ClimaMind personnel and approved collaborators; encrypted transport is used for application and system-to-system transmission.
Confidential	Customer site metadata, building telemetry, dashboard data, diagnostics, support context, customer configuration	Access-controlled; encrypted in transit and at rest; used only for customer delivery, support, operations, and approved analysis.
Restricted	Credentials, secrets, device identity material, BAS access details, control-write authorization data	Stored in AWS Secrets Manager; encrypted in transit where transmitted; access is tightly restricted.

Customer data retention and deletion are handled by data class and customer agreement. When customer deletion or return requests apply, ClimaMind routes them through a documented operational process.

Edge Device Security Model

ClimaMind treats edge deployments as a controlled security boundary with three security surfaces: communication with ClimaMind cloud services, communication with customer BAS systems, and local device runtime protection.

Internet and cloud communication:

- production edge-to-cloud communication uses encrypted transport and certificate validation;
- telemetry ingestion from edge devices is authenticated or signed;
- telemetry payloads preserve device identity, timestamp, sequence, and operational context for traceability;
- upload failures use retry and backoff behavior without bypassing authentication;
- production model and configuration updates are versioned and use approved artifacts;
- model, configuration, and control updates are validated and have rollback practices.

BAS communication:

- edge devices connect only to customer-approved BAS endpoints or gateways;
- customer site connectivity is constrained through approved network placement, routing, ACLs, or gateway configuration;
- BAS writes are limited to allowlisted production control points;
- control writes follow least-privilege access;
- control paths fail closed when device identity, source snapshot, model/configuration version, manifest, or write target cannot be verified.

Building control safety:

- customer BAS sequences, operator actions, equipment safeties, lockouts, and life-safety controls remain authoritative;
- ClimaMind does not bypass customer-defined safety limits, interlocks, overrides, or equipment protection logic;
- writable BAS points are mapped, reviewed, and approved with customer IT/OT before production use;
- control writes are bounded by approved operating ranges, write cadence, and deployment-specific control strategy;
- control decisions require valid, recent, and bounded telemetry; stale, missing, inconsistent, or out-of-range source data triggers no-write or customer-approved fallback behavior;
- when communication, validation, model/configuration, or BAS write confirmation fails, the edge device stops issuing new control writes and leaves the customer BAS in control;
- production enablement follows a customer-approved commissioning path such as point-map review, read-only observation, limited write testing, and customer sign-off;
- rollback can disable edge writes or revert the active model/configuration without requiring changes to the customer's underlying BAS sequence;
- each BAS write attempt records the site/device identity, source snapshot, model/configuration version, target point, requested value, accepted/rejected result, and reason where available.

Local edge runtime protection:

- production edge devices use unique site and device identity;
- field-device values must reflect authorized deployment sources;
- local runtime changes are limited to approved model/configuration artifacts and deployment components;
- malware and unauthorized runtime changes are mitigated through restricted local access, controlled software updates, and runtime monitoring appropriate to the deployment;
- telemetry uploads, control decisions, model/configuration versions, source snapshots, and write results are auditable.

Customer-Controlled Deployment Responsibilities

Customer review may involve IT, OT, facilities, engineering, security, or other site stakeholders depending on the customer's operating model.

For building deployments, customer IT/OT approval defines the allowed BAS endpoints or gateways, network placement, routing, ACLs, gateway configuration, and any site-specific logging or evidence destination.

Customer-provided BAS credentials or access paths are scoped to the approved deployment purpose and allowlisted control points. Remote support access, when used, is approved by the customer for a defined support window.

Remote Support Access

Remote support is not enabled as a default trust path. Routine operations rely on telemetry, health status, logs, and controlled model/configuration updates.

When remote support is required, access is customer-approved, time-bound, source-restricted, certificate-authenticated, least-privilege, and logged. Remote support access does not replace device identity, authenticated telemetry, allowlisted BAS writes, or fail-closed controls.

Onsite support can be used where customer policy does not allow remote support access.

Audit Records

ClimaMind maintains audit records for production-relevant actions, including:

- user access to customer-facing dashboards;
- edge telemetry uploads and ingestion results;
- model/configuration versions delivered to edge devices;
- control decisions, allowlisted BAS write attempts, and write results;

- remote support access approvals, access windows, and session activity when remote support is used;
- production access, deployment, recovery, and incident response actions.

Audit records are stored in ClimaMind's cloud logging environment or, where agreed with the customer, in a customer-designated logging or evidence location.

Access Control

ClimaMind's production access model is designed around least privilege and named-account access. Privileged access has a business purpose and is reviewed periodically.

Production credentials are provisioned through controlled channels and scoped to their intended use.

Production edge connectivity is scoped to the minimum required customer-approved network paths. Customer building-system access is limited to authorized deployment components.

Change Control

Changes that affect customer data, production deployments, edge device identity, building control paths, credentials, customer-facing availability, or production security controls are subject to release validation and rollback practices.

Security-relevant dependencies, container images, and software components are reviewed and remediated based on severity, exploitability, and customer impact.

Availability And Recovery

Production-impacting systems have rollback or recovery procedures appropriate to their customer impact. High-impact deployment changes preserve a mitigation path, and backup or restore practices are reviewed for systems that store customer data or production configuration.

Incident Response

ClimaMind maintains an incident response approach covering detection, triage, containment, recovery, customer impact assessment, remediation, and post-incident review.

Security events that may require escalation include:

- unauthorized production access;
- credential exposure;
- customer data sent to the wrong environment;
- incorrect site or device identity usage;
- unauthorized or unexpected building-control writes;
- multiple writers affecting the same site/device;
- field deployment connected to an unauthorized component.

Vendor Risk

Vendors and subprocessors that process customer data, support production operations, or access sensitive production systems are reviewed for security posture, data access scope, contractual protections, and available security documentation. Where applicable, customer data processing is governed through contractual terms such as a data processing agreement.

Supporting Materials Available On Request

Depending on customer review needs, ClimaMind can provide supporting materials such as data retention details, vendor or subprocessor information, data processing terms, customer responsibility matrix, site-specific network approval records, commissioning records, and audit evidence exports.