

نظرة عامة على أمن العملاء

يلخص هذا المستند حدود أمن ClimaMind، وضوابط النشر، وتدابير حماية بيانات العملاء لأنظمة الإنتاج ذات الأثر على العملاء.

صممت ClimaMind للنشر الآمن في بيئات مباني العملاء، مع اتصال مضبوط من الطرف إلى السحابة، وربط BMS يعتمد على العميل، وسجلات تشغيل قابلة للتدقيق. هذا الملف مادة مراجعة لفرق IT و OT والأمن والمرافق. وهو ليس ادعاء اعتماد.

هندسة النشر

يبقى مستخدمو العميل، وخدمات ClimaMind السحابية، وبيانات الموقع، وجهاز الطرف، وBMS الخاص بالعميل منفصلين عبر مسارات إنتاج صريحة.

- يصل مستخدمو العميل إلى dashboard عبر TLS.
- يتحقق Secure Cloud Gateway من اتصال الطرف والتحديثات المعتمدة.
- تخزن بيانات الموقع في خدمات ClimaMind السحابية وتفصل عن مسارات التحكم في BMS الخاص بالعميل.
- تتصل أجهزة الطرف بخروجا بخدمات ClimaMind؛ ويبقى BMS داخل موقع العميل.

تصنيف البيانات ومعالجتها

المعالجة	أثناء النقل	في التخزين	أمثلة	التصنيف
معتمد للتوزيع الخارجي.	لا	لا	محتوى الموقع العام والوثائق المنشورة	Public
ClimaMind والمتعاونين المعتمدين. مقصور على موظفي	نعم	لا	ملاحظات تشغيلية غير عامة وتفاصيل تنفيذ	Internal
والدعم والتشغيل والتحليل المعتمد فقط. وصول مضبوط؛ للاستخدام في التسليم	نعم	نعم	الموقع والقياس و dashboard والتشخيص والتهيئة بيانات وصف	Confidential
AWS Secrets Manager؛ والوصول مقيد بشدة. مخزنة في	نعم	نعم	والأسرار وهوية الجهاز ووصول BMS وتفويض الكتابة بيانات الاعتماد	Restricted

حماية البيانات

يركز أمن النشر على بيانات الموقع، ووصول dashboard، والتهيئة التشغيلية، وقياس الطرف عن بعد.

- يعامل الموقع العام ومواد النظرة الأمنية المنشورة كمعلومات عامة.
- تعامل الملاحظات التشغيلية غير العامة وتفاصيل التنفيذ كمعلومات داخلية.
- تعامل بيانات وصف الموقع، وقياس المبنى، وبيانات dashboard، والتشخيص، وسياق الدعم، وتهيئة العميل كمعلومات سرية.
- تعامل بيانات الاعتماد والشهادات و API tokens ومواد التوقيع كأسرار مقيدة وتحفظ في AWS Secrets Manager.
- الوصول الإنتاجي قائم على الأدوار ومحدود بالحاجة التشغيلية.

أمن جهاز الطرف

يستخدم جهاز الطرف اتصالا سحابيا خارجا ومصادقا عليه، مع مسار تحديث ضيق.

- يستخدم جهاز الطرف اتصالا خارجا فقط إلى نقاط نهاية ClimaMind السحابية المعتمدة.
- يحمي TLS والتحقق من الشهادات الاتصال السحابي.
- يستخدم رفع القياس اتصالا مصادقا عليه وموقعا.
- تسليم التحديثات مصدر بإصدار ويستخدم مسارا مصادقا عليه مع إمكانية التراجع.
- تحد تهيئة التشغيل المحلية الخدمات إلى الدور المطلوب في موقع العميل.

سلامة التحكم في المبنى

يقتصر اتصال BMS على المسارات والنقاط التي يعتمدها العميل، مع سلوك تحكم محدود.

- يقتصر الاتصال على نقاط نهاية BMS وتعيينات النقاط التي يعتمدها العميل.
- يدعم النشر براءة أولا التحقق قبل أي إجراء تحكم.
- كتابات BMS على allowlist ومقيدة بالنقاط المعتمدة.
- تحافظ إجراءات التحكم على سلطة BMS المحلية، وسير عمل المشغل، وقيود التشغيل التي يحددها العميل.
- يحافظ سلوك التراجع fail-safe على تشغيل المبنى القائم.

وصول الدعم عن بعد

الدعم عن بعد صريح، ومحدود زمنيا، ومتوافق مع سياسة موقع العميل.

- لا يلزم نفق إدارة عن بعد دائم للنشر العادي.
- لا يلزم مسار VPN أو SSH أو RDP دائم افتراضيا للنشر.
- يستخدم الدعم موافقة العميل ويمكن أن يعتمد على عنوان IP مصدري ثابت، أو التحقق من الشهادة، أو الوصول في الموقع.
- تعتمد جلسات الدعم للمهمة والنافذة الزمنية وتسجل.

سجلات التدقيق

تسجل الأحداث ذات الصلة بالأمن في أنظمة ClimaMind السحابية أو في موقع أدلة يحدده العميل عندما يتطلب النشر ذلك.

- مصادقة dashboard والوصول الإداري.
 - تغييرات تهيئة النشر وتحديثات النموذج أو التهيئة.
 - حالة رفع القياس، وأحداث تسليم التحديثات، وأحداث المصادقة بين الطرف والسحابة.
 - محاولات كتابة BMS، وإجراءات التحكم المعتمدة، وجلسات الدعم عن بعد.
- تدعم هذه النظرة مراجعة المورد، واستقبال الأمن، وتخطيط النشر دون كشف مسارات التنفيذ الداخلية.