

Crop Urbanis Security and Data Boundaries

Current public/private boundaries and selected-scope requirements

Canonical status version	status-2026-08-26
Publication	26 August 2026

Security and data boundaries for the current Platform and selected beta scopes.

The public website, internal Platform work and any selected organisational beta environment are separate data contexts. This page states current controls and planned hardening without claiming certification.

Public forms accept high-level context only.

The public website does not create a Platform account or workspace. Detailed or confidential material is exchanged only after scope, data route and responsible parties are agreed.

May be submitted

Contact details, organisation, role, country and high-level project or collaboration context.

Must not be submitted

Confidential files, supplier-confidential documents, credentials, detailed financial models, special-category personal data or regulated operational data.

Implemented controls are distinguished from hardening work.

Controls are assigned to the applicable environment and scope; none is presented as a certification.

Public-site minimisation

No public account creation or file upload; high-level contact data only.

Scoped access

Any selected beta scope requires named users, roles, purpose, data categories and responsible contacts before access.

Transport and secret handling

Encrypted transport and managed secret handling are required for the agreed deployment; at-rest encryption is used where supported by the selected service.

Logging, backup and lifecycle

Auditability, backup, recovery, retention, export and deletion behaviour must be fixed for the selected scope before production use.

Provider, region, retention and training conditions are scope decisions.

The public site currently uses Cloudflare Pages, Web3Forms for form forwarding and an optional Calendly scheduler. Any selected beta environment must document the actual infrastructure and model providers, regions, subprocessors, retention and training conditions before confidential data is processed.

No public-model training by default

Confidential beta data is not used to train public models unless separately authorised in writing.

Purpose limitation

AI processing is limited to the agreed task and permitted data categories.

Scope and data conditions precede access.

Before access, agree organisation, authorised users, roles, purpose, capability scope, source rights, confidentiality, provider and region choices, subprocessors, retention, export, deletion, support, incident contact and professional responsibilities.

Security controls do not transfer professional authority.

Organisations and relevant professionals remain responsible for their technical, legal, regulatory and operational decisions. Crop Urbanis does not claim a security certification unless formally obtained and named.