Who Owns What: The AtlasOA Shared Responsibility Model

The architecture

AtlasOA runs on hardware your institution operates. There is no AtlasOA LLC cloud, no AtlasOA LLC server farm, no AtlasOA LLC database. Your assessment data, your accreditation evidence, and your program review records live on your server. We never see them. That is the central trade of the on-premises model: you get full control of your data, and in exchange you operate the server it lives on.

Because of that architecture, security and incident response are divided between two parties. This page lays out who owns what so your IT team and your CISO can match AtlasOA to how they already run other on-premises platforms like Banner, Workday, or your SIS.

AtlasOA LLC (the vendor) is responsible for

1. Code-level security of the AtlasOA software. Every release goes through automated tests, internal security review, and adversarial code review before shipping.
2. Timely patching of vulnerabilities found in the codebase. Critical fixes within 7 calendar days, high-severity within 30 days.
3. Secure defaults in the installer. Role-based access control, CSRF protection, brute-force lockout, password hashing, and session timeouts are on out of the box.
4. Coordinated disclosure to all institutions when a vulnerability is found that affects more than one customer.
5. 72-hour notification of any unauthorized access involving the AtlasOA codebase, AtlasOA LLC vendor systems, or AtlasOA LLC personnel. Notification includes the nature and scope of the incident, the categories of student or institutional data affected, and the mitigation steps in progress.
6. Hardening guides, deployment runbooks, and an incident response template that your IT team can adapt to your institution.

Your institution (the customer) is responsible for

1. The server, OS, perimeter, full-disk encryption, and backups. AtlasOA runs on your hardware; the operating system, firewall, BitLocker, and backup operations are your IT team's normal responsibility.
2. User account provisioning and deprovisioning inside AtlasOA. When faculty and staff arrive, leave, or change roles, your administrator updates AtlasOA the same way they update any other on-premises system.
3. Applying AtlasOA security patches within a reasonable window after release, consistent with the severity advisory issued by AtlasOA LLC.
4. Monitoring the AtlasOA audit log and your campus network for indicators of unauthorized access. The AtlasOA admin UI exposes the audit log; your IT team uses their existing monitoring tools and processes.
5. 72-hour notification to AtlasOA LLC if your institution discovers an incident involving AtlasOA data, so AtlasOA LLC can investigate root cause and, if applicable, issue a coordinated disclosure to other affected customers.
6. Notifying students, faculty, accreditors (regional and program-specific), state Attorneys General, and any other regulators as required by your institution's own statutory obligations under FERPA, the Gramm-Leach-Bliley Act safeguards rule, applicable state student privacy and data breach notification laws, and your accreditor's institutional integrity or substantive change rules.

When something goes wrong on shared ground

Some incidents have shared root causes spanning both the AtlasOA codebase and your institution's deployment environment. When that happens, AtlasOA LLC and your institution will cooperate in good faith on root cause analysis, remediation, and notification timing. AtlasOA LLC's cooperation is limited to technical guidance about the AtlasOA software's behavior, because AtlasOA LLC does not, under normal operation, have access to any of your data.

The legal version

The full text of this division lives in Section 4A of the AtlasOA Data Processing Addendum, which AtlasOA LLC shares under NDA during procurement. Section 5 of the same DPA is the formal 72-hour vendor-side breach notification commitment.

Why this matters

Shared responsibility is the standard model for every on-premises higher-ed software vendor. Institutions operate the server, vendors maintain the software. AtlasOA is explicit about the model so there is no ambiguity at procurement time and no surprises during an incident.

AtlasOA LLC | 8112 Maryland Ave, Suite 400, St. Louis, MO 63105 | ashleyreddick@atlasoa.com | atlasoa.com