Who Owns What: The Atlas K-12 Shared Responsibility Model

The architecture

Atlas K-12 runs on hardware your district operates. There is no AtlasOA LLC cloud, no AtlasOA LLC server farm, no AtlasOA LLC database. Your student 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 Atlas K-12 to how they already run other on-premises platforms.

AtlasOA LLC (the vendor) is responsible for

1. Code-level security of the Atlas K-12 software. Every release goes through automated tests, internal security review against the OWASP Top 10, 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 districts when a vulnerability is found that affects more than one customer.
5. 72-hour notification of any unauthorized access involving the Atlas K-12 codebase, AtlasOA LLC vendor systems, or AtlasOA LLC personnel. Notification includes the nature and scope of the incident, the categories of student 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 district.

Your district (the customer) is responsible for

1. The server, OS, perimeter, full-disk encryption, and backups. Atlas K-12 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 Atlas K-12. When staff arrive, leave, or change roles, your administrator updates Atlas K-12 the same way they update any other system.
3. Applying Atlas K-12 patches within a reasonable window after release, consistent with the severity advisory issued by AtlasOA LLC.
4. Monitoring the Atlas K-12 audit log and your network for indicators of unauthorized access. The Atlas K-12 admin UI exposes the audit log; your IT team uses their existing monitoring tools and processes.
5. 72-hour notification to AtlasOA LLC if you discover an incident involving Atlas K-12 data, so AtlasOA can investigate root cause and, if applicable, issue a coordinated disclosure to other affected districts.
6. Notifying parents, students, regulators, and law enforcement as required by your district's own statutory obligations under federal and state law.

When something goes wrong on shared ground

Some incidents have shared root causes spanning both the Atlas K-12 codebase and the district's deployment environment. When that happens, AtlasOA LLC and the Educational Agency cooperate in good faith on root cause analysis, remediation, and notification timing.

The legal version

The full text of this division lives in Section 4A of the Atlas K-12 Data Processing Addendum, which AtlasOA LLC shares under NDA during procurement. Section 5 of the same DPA is the formal 72-hour breach notification commitment.

Why this matters

Shared responsibility is the standard model for every on-premises ed-tech vendor (PowerSchool on-prem, Skyward, Veracross, every SIS). Districts operate the server, vendors maintain the software. Atlas K-12 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