Our security processes

acumen

Security Certifications

Acumen conducts a variety of audits to ensure continuous compliance with industry standard best practices.

Acumen has a certification for compliance with ISO/IEC 27001:2013. An independent body has audited our compliance with this standard and issued our ISO 27001:2013 certificate. Acumen's compliance with this internationally-recognised standard and code of practice is evidence of our commitment to information security at every level of our organization, and that our security program is in accordance with industry leading best practices.

GDPR

We know that maintaining GDPR & privacy compliance is a top priority for your business. That's why Acumen takes a holistic and personalized approach to compliance, maintaining GDPR compliance ourselves, and enabling your business to set its own compliance preferences, as a controller.

Acumen employs data protection and privacy by design, combining enterprise-grade security features with comprehensive audits of our policies, applications, systems, and networks.

Acumen's security team includes a Data Protection Officer (DPO) and Security Lead who continuously ensure that Acumen's practices and products comply with GDPR and similar regulations. Our privacy policy is up-to-date and reflects our GDPR readiness.

Acumen's privacy policy: https://www.acumenci.com/privacy-policy

Data Centre and Network Security

Acumen hosts all its software in Microsoft Azure facilities around the world. Azure provides an extensive list of compliance and regulatory assurances, including SOC 13, and ISO 27001. See Azure's compliance and security documents for more detailed information.

All of Acumen servers are located within Acumen's own protected environment by restricted security groups allowing only the minimal required communication to and between the servers.

Acumen conducts third-party network vulnerability scans at least annually.

Application Security

Web application architecture and implementation follow OWASP guidelines.

In addition to Acumen's extensive testing program, Acumen conducts application penetration testing by a third-party at least annually.

Single sign-on (SSO) allows you to authenticate users without requiring them to enter login credentials for your Acumen instance. Login using Acumen can be disabled, and Acumen supports SSO.

Acumen login requires strong passwords. User passwords are salted, irreversibly hashed, and stored in Acumen's database. Audit logging lets administrators see when users last logged in and when passwords were last changed.

Data Security

All connections to Acumen are encrypted using SSL, and any attempt to connect over HTTP is redirected to HTTPS. All data is encrypted at rest and in transit.

Data access and authorizations are provided on a need-to-know basis and based on the principle of least privilege. Access to the Azure production system is restricted to authorized personnel and is carried out using VPN with Active Directory authentication.

Security Policies and Secure Development Life Cycle (SDLC)

Acumen maintains security policies that are maintained, communicated, and approved by management to ensure everyone clearly knows their security responsibilities.

Code development is done through a documented SDLC process. Design of all new product functionality is reviewed by the Acumen security team. Acumen conducts mandatory code reviews for code changes and periodic in-depth security review of architecture and sensitive code. Acumen development and testing environments are separate from its production environment.

Employee hiring process includes background screening.

Application Monitoring

All access to Acumen applications is logged and audited.

Logs are kept for at least 90 days.

Acumen maintains a formal incident response plan for major events.

acumen