

Acumatica Security Advantages

Acumatica is designed to satisfy the security needs of banks, health-care and government organizations. All business logic and processing is done on a server in a secure location of your choice. All information received from a user's browser is verified before being accepted and written to the database. Data transferred over the Internet and data stored in the database is encrypted.

Top 10 reasons why Acumatica is more secure than the competition

You control where data is stored and processed

Unlike many web-based applications, with Acumatica you are in full control of where your data is kept and processed, and you are in full control over who has access to maintain and use your system. Acumatica can be installed at your location or at a Hosting or Cloud Services provider. Hosting providers offer 24x7 staff in physically secure data centers that exceed what most businesses can provide internally - and often at lower cost. For some organizations however, data and processing must be performed internally at locations mandated by governmental or corporate policy. With Acumatica the choice is yours.

Server processing

With Acumatica all business logic is processed on the server and not on the user's computer or in a web browser. Unlike some applications that process business logic in the browser, all calculations, validations, and reports are all processed on the server. Since the business logic never leaves the server, there is less chance for anyone to learn how your system works.

Strong user authentication

User logins can be limited from specific IP addresses. You can define how long user passwords must be, and how often they must be changed. The user's browser session times out automatically after a period of inactivity which you define. You can optionally install One Time Password (OTP) systems that issue new passwords every few minutes and that are linked to the user's cellular phone or to a small device that can be attached to a key chain.

Data is kept only on the server

Customer, vendor, employee files, transactions, wiki pages, and all other data remain on your server. As users complete forms only the small bits of data they actually see is transferred to the web browser - and even only then for a brief instant. Once forms are completed no data remains in the browser, and data is never stored on the user's computer.

Encrypted communications

To transfer information between Acumatica and the user's browser, Acumatica uses https, the same encryption technology used by banks to insure no one can 'listen in' on your data. With Acumatica there is no performance penalty for using https.

Database encryption

To protect especially sensitive information Acumatica encrypts certain fields such as credit card numbers, social security numbers, names and rates of pay, within the SQL database. This protects you in the event a backup copy of your information is lost or stolen. You can designate whatever fields you wish to be encrypted in this manner.

Menus display only authorized screens, reports and pages

User menus display only the applications and pages authorized for each person. This also reduces the complexity of the application for individuals and speeds learning.

User screens and reports display only authorized information

Data items that are not authorized for a user will not be displayed on forms or reports. Popup inquiry screens that help users fill out forms only display items the user is authorized to view.

Role based user security

Security policies can be assigned by Role which reduces the number of security settings and the chance for error. An unlimited number of Roles can be created, so there is no limit on the types of security rights granted.

Re-validation within a single user session

Each transmission between the browser and the application server is re-validated from an encrypted key