Security System

Business Value

Our top priority is to provide a 100% hazard-free and trustworthy service. We are constantly focusing our efforts on maintaining our product's infrastructure, technologies, and procedures to be able to guarantee a secure and reliable working environment.

Your employees' personal details, project-related information, files, documentation and any other interactions within our system are fully backed up and protected. Access to each system, network device, and application is limited to authorized personnel, and logged in detail with event logs that are reviewed on a regular basis.

Designed around a multi-tiered architecture that is recommended for web-based applications, the architecture partitions application functionality into independent layers: the presentation layer (or browser client), the business logic (application server) and the data layer (database).

The presentation layer never communicates directly with the database layer. All communication is performed via the business logic, which provides its own security checks before permitting access to the data. This prevents requests from a web browser going directly to the database. The application also verifies the user role at every request.

WebAtlante makes use of strong encryption to protect customer data (which is stored on an encrypted file system) and communications, including SSL Certification. SSL (Secure Sockets Layer) is the standard security technology for creating an encrypted link between a web server and a browser. You will know you have created an SSL link when the URL is in green, begins with "https://" and there is a padlock symbol either at the beginning or end of the URL.

Secure mechanisms are used to verify the identity of users attempting to access the system. In order to access the system, the user must enter a username (e-mail address) and password.

Passwords are protected using sophisticated hashing and salting techniques; We only ever stores hashes of password, never the passwords themselves.

Key Features

- Regular maintenance and system updates
- High-standard network protection procedures
- Authentication and access control
- Secure and reliable data storage
- Continuous storage back-up