



CLARIZEN SECURITY

At Clarizen, we consider security to be a business imperative and a critical component to successfully managing your projects online. That is why we made it an integral part of our solution's architecture.

- State of the art technology, combined with strict procedures protects your privacy and keeps user information, documents and data confidential
- Clarizen's solution architecture is designed to safeguard against security breaches – no matter the source (hacking, spying, phishing)
- We guarantee our service availability and reliability, ensuring no service or data loss; the Clarizen project management service is accessible anywhere, at anytime

FACILITIES & DISASTER RECOVERY

- Clarizen's server farms are hosted at a Tier 1 location in California
- The facility is SAS 70 Type II certified
- To protect our customers' data, ensure service reliability and availability Clarizen utilizes two mirrored data centers
- The entire data is replicated in real time to a disaster recovery and backup site, hosted on a secured facility on the East Coast of the United States

INFRASTRUCTURE

Clarizen ensures all communications going to and coming from its servers are secure.

- Clarizen utilizes a multi-tiered network security infrastructure to prevent security violations

- We employ data encryption to ensure your data is kept private and secure. Multiple firewalls and network scanners further secure all access to our servers and prevent hacking.
- Clarizen regularly performs penetration testing and deploys the latest security updates to guarantee our system is always protected against new threats
- Application Firewalls further protect the system by preventing any malicious activity within the application. Clarizen uses complex algorithms to make sure that the application is not manipulated in any way that may cause harm to your data
- Additional mechanisms such as anti-virus and application monitoring are put in place to protect against malicious hacking attempts
- Clarizen's project management service is constantly monitored to make sure that any out of the ordinary activities or failures are immediately reported. Several alert mechanisms are in place to escalate any such occurrences
- Clarizen also undergoes ongoing penetration testing audits by multiple credible third party security testing firms
- Backup is performed in a multi layered fashion having both local and off site backups running at all times – the offsite backup is kept at Clarizen's disaster recovery site

PROTECTING YOUR ORGANIZATION'S DATA

The security and protection of your organization's data is paramount.

- Clarizen ensures that information is kept secure and private by preventing unauthorized users to access your data
- Clarizen security mechanisms ensure your project data is accessible only to registered users belonging to your organization

USER AUTHORIZATION AND ROLES

- Each user has a unique username and password that must be entered at the start of each Clarizen session. All passwords are stored in encrypted MD-5 hash format
- Clarizen secures user IDs, passwords and other user information such that they are never jeopardized
- Clarizen's role and authorization mechanisms ensure that data access and user actions can be limited by each user's role in each project
- Project managers have the capability to assign roles in their projects to specific users and grant them permissions as required

ABOUT SAS 70

SAS 70: Statement on Auditing Standards No. 70. SAS 70 is an "internationally recognized auditing standard developed by the American Institute of Certified Public Accountants" (AICPA). According to "Service Organizations: Applying SAS No. 70, as Amended – AICPA Audit Guide," "a SAS 70 audit ... is widely recognized, because it represents that a service organization has been through an in-depth audit of their control activities, which generally include controls over information technology and related processes." There are two types of Service Auditor's Reports: Type I and Type II. Type II reports include the "service organization's description of controls, [and] also includes detailed testing of the service organization's controls over a minimum six month period."