Secure Collaboration on your Projects with Teamwork.com

Over 100,000 companies worldwide in 147 countries trust Teamwork.com to manage their projects in the cloud - and we take this trust very seriously. Our top priority is to ensure that your project-related data remains secure and confidential, and we adhere to the highest professional security standards to do so. Our goal is to provide you with an easy-to-use, flexible, and scalable project management application with dependable service and comprehensive security at all levels. And we succeed at this -- we've never had a security breach or lost customer files. To keep our environment secure, we constantly focus on maintaining the reliability of our product, infrastructure, technologies, and procedures.

Our security model consists of three elements: physical, network, and content. Here's how we deal with each of them.

Physical security

We host Teamwork.com within the Amazon's Web Services (AWS) environment. These are world-class data centers and we make use of their web/application servers, file servers and databases. The Teamwork.com system spans several layers of the AWS in that we utilize the Elastic Computing (EC2) for our application and web servers, and additionally for other file servers. The File servers are connected to the AWS Storage facility (S3), while the application is connected to the Relational Database System (RDS).

Key to all of our security measures is the physical security of the AWS data centers. The buildings that house the centers have significant physical access control, and incorporate extensive seismic bracing as well as the latest smoke and fire early-detection systems. The sites are monitored constantly, 24x7x365, by digital surveillance systems.

The digital security of our system and your information resides behind the AWS firewall, Spam and DOS protections, and is only visible to specifically monitored IP addresses. In effect, you connect to Teamwork.com through an AWS load-balancer via the AWS network, so it shouldn't matter where the computers are. But for reference, Teamwork.com straddles multiple 'zones' in the Virginia AWS Data Center (a short walk away from the AWS U.S. Government servers).

The third element of the physical security of your data is backups. At the AWS data centers, all the databases are backed up twice a day by one of the file servers and then backed up to the S3 storage. The RDS Databases are configured to point-in-time recovery, up to the last 5 minutes, within the previous 3 day period, and snapshots of the Database servers are taken every morning (GMT). All primary database servers have fully replicated slaves and are always in sync. The Application and file servers are snapshot on a regular schedule.

Along with the backups comes the ability to restore the data if needed, and our customer care team can help you with this.

So, the physical location is secure, your data is safe behind firewalls and spam protections, and you can retrieve anything from the data backups. But what of uptime, the security of being able to access your projects on Teamwork.com whenever you want to?

In **6 years** of continuous service, Teamwork.com's uptime has consistently exceeded 99%. Running Teamwork.com in the AWS environment, compared to a more traditional ISP hosting provider, means that all services are essentially virtual, and so are not vulnerable to physical hardware failures. Yes, we are sharing the AWS environment with many other companies, but sharing resources is what is contributing to our outstanding uptime percentage.

Network security

Network security consists of two elements that both need to be considered: the security of the infrastructure itself and then of the data within it.

Industry standard protection procedures for our network infrastructure are an integral part of Teamwork.com's engineering culture. Between us, we have many years of experience with protection mechanisms such as firewalled servers and alert mechanisms. But these specifics are based on years of experience, and a deep understanding of the entire picture of network security: operations, back end, front end, and social engineering. Appreciating the whole scope gives us the edge in our security measures.

The other side of network security is data protection, and at Teamwork.com we encrypt all your data with 256-bit Secure Socket Layer (SSL) with the RC4 algorithm and 2048-bit key length. You're secure on two fronts as, when you access Teamwork.com, SSL technology protects your information using both server authentication and data encryption. This is equivalent to the data security methods used in banking and leading e-commerce sites. And we don't play favorites with our data encryption - it's the same across the board, whatever your subscription type.

With the network secure and your data encrypted, we now turn to the security of the content of your files.

Content security

Content security revolves around who has access to your data, whether it's our staff running the data center infrastructure or your project team members who you give access rights to. We'll start with us.

The Teamwork.com team members have years of experience in designing and operating data centers, as well as in continually improving the processes that aren't working so well or that can be adjusted to work more efficiently and effectively. Based on all our experience, we've developed world class practices for managing security and data protection risk. We strongly believe that designing and running a data center infrastructure requires not just technology, but a disciplined approach to the processes involved -- escalation, management, knowledge sharing, risk, as well as the day-to day-operations.

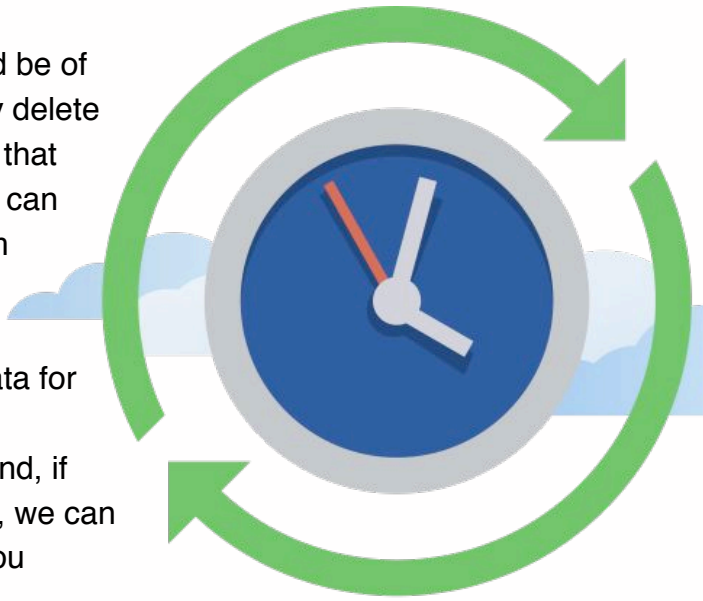
It's not just our wealth of experience that sets us apart from other companies in this area -- it's also our philosophy of teamwork. We have Team Members, not employees. An employee is a pawn to be sacrificed, a team member will have your back. We know all members of our team personally, and they have the highest clearance to access the data center data. That said, we also strictly regulate access and passwords to those few team members who need to access the customer data for troubleshooting or to provide support, and we keep a log of all such access. And even then, we won't go into your data without your permission (perhaps as part of a support incident), and into the data center data only on the go-ahead from senior security management for support and maintenance.

And now about you. You control access to your data on Teamwork.com through user authentication and user rights.

User authentication ensures that only valid users can get into your project management system. Each user in Teamwork.com has a unique account protected with a password. This account is tied to a verified email address that must be entered when a user logs in. For additional security, you have the option to require that passwords be high-security alphanumeric passwords.

Once in to Teamwork.com, each user is limited in actions to those assigned to her by the Teamwork.com Project Administrator through user level granular, rights and permissions, settings. Permissions allow a user to perform certain actions and activities within Teamwork.com, such as adding and editing tasks, or deleting files. The Administrator and Project Administrator have the power to determine who can do what in which project.

Content security is also about who can see what kinds of data in your Teamwork.com projects. Your project and tasks are accessible only to you unless you explicitly share the data with someone else in your account, or place the information in a shared Notebook.



And the security of your data content itself should be of concern to you. What happens if you accidentally delete something, or later decide that you do need data that you've gotten rid of? We've covered this too. You can safely recover the accidentally deleted items from Teamwork.com's recycle bin at anytime. And, just in case you've tidied up and emptied your recycle bin, we keep a backup of the removed data for approximately two weeks. Contact our customer support team in this period to restore it for you. And, if you delete a user who you later want to reinstate, we can do that too, along with all her tasks, as long as you contact us within a month.

Would you like to know more?

For further details on how Teamwork.com collects and processes your information, please refer to our Privacy Policy. To learn more about how Teamwork.com's service is delivered, please read our Terms of Service. If you have any questions about the security of Teamwork.com, contact us anytime at support@teamwork.com and we'll get back to you quickly.