ProjSync Security Whitepaper

ProjSync enables centralized data tracking and sharing so that all stakeholders have up-to-the-minute information about every aspect of the project.

Gadzoom prioritizes security in both development and operation of the ProjSync software suite. This ensures the safety of confidential data and allows clients to give or remove access to project participants at will.

The purpose of this document is to give an overview of the data and operational security of ProjSync, not general features of the software.

Unless otherwise noted, all security features discussed apply to the entire ProjSync suite of software.

Infrastructure

Our servers are hosted with Amazon Web Services and have the outstanding physical security that AWS is known for. For a summary of AWS data centers' physical controls, see:
https://aws.amazon.com/compliance/data-center/controls/

Our deployment process is automated and allows minimizing dependencies and up-to-date patching of the ProjSync software and dependencies, including the operating system layer.

Infrastructure, such as databases, are not accessible to the public internet.

ProjSync infrastructure uses the principle of minimum privileges. If a staff member does not need access to a resource, then they do not have access to that resource.

Authentication & Identity Management

Access to ProjSync is controlled through authentication of a user profile using a username and password. User profiles are managed by the client's company account including administration of credentials, permissions, and configuration of credential requirements.

Multi-factor authentication is planned for the near future; when it is released, there will be an option to require multi-factor authentication for user profiles in the company.

Administrative Controls / Permissions

ProjSync has a role based permission system to allow granular permissions to be given to individual profiles to limit sensitive information to only those personnel which require access. Employees can be given Roles on a Project which define the permission level they require on that project; this allows easily giving and removing permissions from an employee according to their current role on specific projects. An employee may have different roles and levels of permissions on different projects. When an employee is removed from a project, all access to information on the project is removed.

Software Development Process

ProjSync software is developed with constant attention to security and a strict policy of code review so that multiple developers are inspecting code for flaws or vulnerabilities before being deployed in production.

Database queries are done using prepared statements and special attention is made to prevent SQL injection attacks. Similar care is taken with other classes of web application vulnerabilities.

Security is treated as part of the design and production process, not as a list of features.

Encryption

ProjSync uses standard SSL / TLS encryption from browser connections to prevent Man-in-the-Middle attacks or interception of data.

Privacy

The privacy of our users is very important and a key part of our approach to security.

- We do not sell your data
- We do not use your data collected during use of ProjSync for advertising purposes

To see our full Privacy Policy, go to: "https://www.projsync.com/legal/privacy-statement.html"