



## Security Policy

Wimi adheres to the highest industry standards for security



SSAE 16 data  
center



99.95%  
Accessibility



SSL 256 (bank  
level security)



Highest industry  
standards

## ✓ **Protection and integrity**

All data in your Wimi is stored in a data center adhering to the highest industry standards and uses a cloud server infrastructure maintained and updated by industry professionals.

More and more organizations with a need to store particularly sensitive data (companies, governments, research labs) are turning to cloud storage. This preference can be attributed to the fact that cloud based hosting solutions offer the highest level of performance and security.

## ✓ **Resilient storage infrastructure**

Wimi has chosen to rely on RAID 10 (RAID 1 combined with RAID 0).

This technology allows data to be stored simultaneously across multiple disks which allows the loss of multiple physical disks before data corruption is possible.

If a problem occurs on one drive, it is immediately replaced and the data is replicated to the new disk.

## ✓ **Accessibility**

Our hosting infrastructure enables us to ensure a maximum accessibility of 99.95%.

In addition, due to the flexibility of the cloud infrastructure, Wimi can deal with very substantial use changes without any slowdowns.

In case of an important incident, connections to the main server will be switched to the secondary server: your data is protected and accessible.

## ✓ **Backing up your data**

Wimi also has secure backup devices of your data.

An incremental backup of data keeps all your data safe on a separate server. Even in case of a serious server failure, your data is protected.

In addition, a real-time replication system to another data center is in place. The secondary data center is geographically distant from the main data center.

## ✓ **Confidentiality**

To ensure the confidentiality of your data when you share with the contributors of a project, Wimi uses digital certificates and uses SSL (Secure Socket Layer).

A digital certificate installed on our servers, enables: 1) Authentication of the server thanks to validation made by the certification authority; and 2) Secure sending and data integrity between the site visitor and the server. Two digital encryption keys are provided: a private key and public key. Wimi keeps the private key secret. The public key is used by our clients in order to communicate with our server.

When an exchange takes place between Wimi and its users, the client browser checks the validity of the certificate, and then establishes an encrypted connection using 256-bit AES (depending on your configuration).