



RASCO – FTP & CLOUD DATA SHARE PLATFORM SECURITY DETAILS

PLATFORM NAME: Zoho WORKDRIVE
CONTRACT TYPE: BUSINESS EDITION
WEBSITE: <https://www.zoho.com/workdrive>

DATA SECURITY DETAILS

INDUSTRY STANDARD DATA SECURITY

Zoho WorkDrive meets industry-specific compliance standards such as SOC 2 Type II and ISO 27001. It uses a defence-in-depth approach to provide security at the physical, logical, and data levels.

Data level security

Zoho's data centers are hosted in secured locations and monitored with night vision cameras, 24*7 throughout the year. Zoho WorkDrive's servers and clients are connected through SSL and secured with an RSA-based 2048-bit encryption key.

Disaster recovery

Zoho servers are well protected from all kinds of physical damage. Zoho servers run on distributed grid architecture. In case of server damage, a copy of your files will be safely backed up in an alternate server and available without any noticeable delay.

Intrusion protection

All files are first checked for viruses before being uploaded and stored in Zoho servers. Our screening uses powerful Intrusion Detection and Intrusion Prevention systems (IDS/IPS) and our systems are secured from DDoS attacks.

Two-factor authentication

Zoho WorkDrive account is protected with a Two-Factor Authentication (TFA). Security means more than just a password. To ensure strong protection, user gets a unique code generated every time he/she logs into an account.



Encryption in transit and at rest

Files in Zoho WorkDrive are encrypted at rest with 256-bit Advance Encryption Standard (AES). During transit, Perfect Forward Secrecy (PFS) generates a unique key for each session to encrypt files.

Transfer file ownership

What's created in an organisation stays in the organization. Transfer of ownership of files from one user to another keeps them in the right hands. It won't let ex-employees leave with the important files they created and worked on.

Shared links that expire and can limit downloads

Data shared is available only for as long as it is wanted to be. Expiration dates can be set on documents while sharing them externally. After the expiration date, external partners won't be able to view the data. Download limits can be set, so the data would be available for download only the number of times as set by the admin.