

How does TrigoldCrystal backup protect data from prying eyes? Data security is essential! You need to protect data against outsiders and against unauthorised internal access.

ENCRYPTION AND PASSWORD PROTECTION

Encryption converts data into an unreadable format to prevent unauthorised viewing or access. Online Pro uses a combination of Blowfish 448 encryption and SSL secure data transmission to ensure the safety of your data.

Password Protection ensures data is protected against access by people who have gained unauthorised access to a PC.

Whether a laptop is stolen or a desktop PC is left unattended, you do not want anyone with physical access to a PC to be able to restore data that was previously backed up. Our Online Backup offers an additional level of security via client password protection. This protection gives you the flexibility to select a private account password (distinct from the encryption key). This password must be entered to restore backed up data. So, even if someone has unauthorised access to a user's PC, they cannot restore backed up data. If a PC is stolen or accessed by unauthorised personnel, a full or partial restoration is impossible.

PREVENTING UNAUTHORISED ACCESS

TrigoldCrystal backup service encrypts all data before it ever leaves your PC, so that it travels over the network to the secure data centres in an unreadable format. It is safe from unauthorised viewing or access throughout both the entire transmission process and the storage interval. Even if unauthorised personnel access transmissions or storage, no intelligible data can be retrieved.

REMOVING THE HACKER THREAT

The software does not create an opening for incoming connections; outgoing connections can be limited to specific ports at specific IP addresses. Therefore, only a client that exists within the corporate trusted network can initiate a session with our secure data centres.

FIREWALL COMPATIBILITY

Our online backup service is compatible with all corporate firewall systems, including SOCKS and proxy servers. Connections are only initiated by clients from within the corporate network. The secure data centres never attempt to connect to a client and thus there is no need to provide an opening in the firewall that would allow external access to your network.

BEST PRACTICES AFFORDS ADDITIONAL PROTECTION

TrigoldCrystal secure data centres are designed to provide extremely reliable protection for your important files. **To this end we employ:**

Transmission Checking: We utilise extensive error checking against data transmitted to the secure data centres to detect transmission problems. Our client software will retransmit any data packets when transmission errors have been detected.

Server Mirroring: We employ two mirrored secure data servers at all times. When data arrives at one, it is simultaneously copied over secure communication lines to the other. By the time the client software ends the backup session, the backup data centre has verified that both copies, one on each redundant machine, have been successfully created.

RAID5 Redundancy: To provide additional insurance against data loss due to disk failure, each computer system in the secure data centres uses self-repairing RAID 5 storage techniques. Inherent to RAID 5 is built in redundancy, which enables the system to automatically recover, without loss of data, from a disk failure. And of course there is always the second copy of the data on the second secure data centre machines