



Tritanium™ Cloud Protection

The cloud backup advantage

Simple

Seamlessly manage backup, sync, and mobile access for multi-user and server environments from a single web-based console.

Secure

Your data is safe with military-grade encryption, world-class data centers, and EMC—a company built to last.

Affordable

Keep costs low with no hardware to purchase and minimal overhead required.

Contact information

Sandra Batakis
25 Goodale Street
Peabody MA 01960
(978) 535-0202 x201
sandra@sandranetwork.com

Powered by Mozy

Our cloud backup Service is powered by Mozy. This paper details the protection and security as it relates to Mozy. Most clouds have a silver lining. Not ours. The Mozy cloud is lined with the triple-protection of Tritanium: military-grade security, state-of-the-art data centers, with the backing of storage leader EMC.

Whether you need to protect data for home, business, or large corporations or educational institutions, Mozy takes every customer's data seriously. Mozy protects and provides secure access to all of your critical files—emails, spreadsheets, presentations—on computers and laptops, and protects mission-critical files on Windows and Mac servers, including support for Exchange, SQL, and file servers.

Don't leave your cloud backup to chance. With more than 100,000 businesses, 6 million customers, and Fortune 500 backing, Mozy has the experience you need.

Military-grade security

Mozy is dedicated to ensuring the safety, security and privacy of your data. As such, we employ military-grade encryption:

- **Data encryption:** When you select a file for backup, Mozy encrypts the file right on your laptop, desktop or server to give you immediate protection with the same encryption standard used by the military (256-bit AES encryption). Files are transferred to Mozy data centers through an SSL-encrypted connection, ensuring that your files are doubly encrypted during transit. This is the same technology used by banks to ensure safe delivery of information online.
- **Data at rest encryption:** Files at rest in the data center also reside in an encrypted state. With a secondary copy of your data remotely stored and encrypted, you have complete protection in case anything happens to your computer or laptop. Mozy customers also have the choice to let Mozy manage the encryption process for them (activating a 448-bit Blowfish encryption key), or you can manage your own key using military-grade 256-bit AES to secure your data during storage.
- **Key encryption:** Mozy offers both AES or Blowfish encryption options including:
 - **Default or standard encryption key:** The default key delivers out-of-the box, secure, ease-of-use encryption for all backups. The default key, also referred to as the standard key, uses the Blowfish algorithm to encrypt the data.



- **Personal key:** Mozy support the use of personal keys by individual users, allowing them to manage their own encryption keys. When using Personal Keys every user specifies their own unique encryption key for the data on their computer. Mozy does not maintain or have any knowledge of that key. So, even under force of law, Mozy cannot decrypt your files if you choose personal encryption.

World-class data management

As a handler of confidential customer data, Mozy is in the business to protect your data.

Mozy has successfully completed the SSAE 16 Type 2 audit, and is ISO 27001 certified. These independent verifications certify that Mozy's processes and procedures meet or exceed the strictest control objectives in the industry.

- **The SOC 1 SSAE 16 Type 2 audit:** SSAE 16 verifies a service organization has been through an in-depth audit of its control objectives and control activities to ensure processing and hosting customer data is done safely and securely.
- **Received ISO 27001 certification:** This is the leading international standard for measuring information security management systems that addresses requirements and best practices to the ever-changing threat scenarios.

Our world-class data centers are SSAE 16 audited and ISO 27001 certified. In addition to a solid infrastructure and 24x7x365 onsite monitoring, our data centers also:

- Require both card and biometric security authentication to enter the facilities and access to our server area.
- Utilize a gas fire suppression system to extinguish fires in the event of an emergency without jeopardizing server functionality.
- Are protected by redundant systems and guaranteed by generators supplied by diesel fuel storage. In addition, multiple network providers service each data center to ensure operation in the event a network carrier fails.
- Have cooling mechanisms in place to ensure the servers are kept at optimal operating temperatures.

Additionally, Mozy aides in compliance with various international standards. Mozy has instituted measures and mechanisms to ensure adherence to the European Union Safe Harbor Privacy Principles. Conforming to the Safe Harbor guidelines, Mozy is subjected to an annual audit for compliance to the seven principles of notice, choice, onward transfer, security, data integrity, access and enforcement. Appropriate employee training and dispute mechanisms are also in place. Furthermore, for those organizations concerned with the privacy of their data, as it applies to the Patriot Act and FISAA 1881a, should ensure that their data is properly encrypted. Data center ownership and location can limit which national and international authorities can access information but only encryption, such as the service from Mozy, offers this level of protection.

A company built to last

Mozy backs up data for 100,000 businesses, over 6 million customers, and manages 90 petabytes of stored information. You can be confident that Mozy has the back-end infrastructure to keep your data safe and secure. As a part of storage leader EMC, Mozy is a key component in EMC's mission of protecting your critical business data. Through our heritage as one of the first cloud computing companies and our partnership with EMC, Mozy has the experience, infrastructure, and financial strength to ensure your data is safe, secure, and available when you need it.