Memeo's commitment to the integrity of its customer data revolves around 3 key tenets: Protection, Backup and Recovery.

Protection

Memeo has implemented state-of-the-art industry systems and procedures to ensure the security and confidentiality of customer data, protect against anticipated threats or hazards to the security or integrity of customer data, and protect against unauthorized access to or use of customer data. Customer account information and access to the Memeo Web Service is accessible only through the use of an individual user ID and password or secure API authorization.

The servers on which information is stored are kept in a controlled environment with limited access. While Memeo will take reasonable efforts to guard personal information we knowingly collect directly from our customer base, no security system is impenetrable. In addition, Memeo cannot guarantee that any passively-collected personal information customers choose to include in documents they store on our systems are maintained at adequate levels of protection to meet specific needs or obligations they may have relating to that information.

Backup

Mission critical application data is stored, backed up and replicated within Memeo's secure data center in Nevada. The standard procedure for data backup is as follows:

- All application data is immediately replicated to a backup database and/or storage repository.
- Application backups will be performed daily and retained for 1 month, at which time the information will be deleted.
- A full application backup will be performed weekly. Weekly backups will be saved for a full year, at which time the information will be deleted.
- The last weekly application backup of the month will be saved as a monthly backup and kept indefinitely. Stale daily and weekly backups will be deleted as per the above stated policies.
- Each application backup will be replicated and synchronized within the data center on a daily basis. Proper environmental controls, temperature, humidity and fire protection, shall be maintained at each location.

All data is stored on RAID 60 compliant platforms. Memeo reserves the right to make exceptions to these policies when justified.

Customer data for Memeo's online backup products is hosted at Amazon's Simple Storage Service (S3). Amazon S3 provides a secure, highly durable storage infrastructure designed for mission-critical and primary data storage. This is addressed in the Data Center section of this document.

Recovery

Memeo has several disaster recovery procedures in place to ensure the timely recovery of mission critical application data. When these procedures are implemented the recovery efforts are prioritized as follows:

- **Customers**: Ensure the integrity of customer data and access to that data after a disruptive event.
- **Assets**: Conducting a damage assessment will determine which assets have been destroyed and/or compromised, which ones are at risk and what resources that are left.
- **Records**: Document the disaster and the corrective actions taken by the Memeo Operations personnel to resolve. This will reduce the likelihood of future events while assessing the responsibility for losses and downtime.

Memeo Backup Client

During the initial backup creation process, the Memeo Backup client allows the user to select an encryption option that will encrypt the data that is backed up. This option cannot be changed once the backup has been created. Memeo uses the military grade, 192-bit Triple DES (3DES) algorithm to encrypt files. Triple DES is the common name for the Triple Data Encryption Algorithm block cipher which applies the Data Encryption Standard (DES) cipher algorithm three times to each data block. Once encrypted, the data can only be unencrypted by a user-defined password.

File encryption provides the strongest possible security for your files because those files can only be unencrypted by using the Memeo client and the user password. If this password is lost, there is no back door available to retrieve the data.

Online Backup

Memeo's online backup feature allows users to protect their most valuable files by sending them offsite to a secure cloud storage infrastructure. Memeo incorporates industry standard security protocols to ensure your data stays safe.

Data Center

The Memeo Online Backup application servers are housed in a secure, fault-tolerant data center. Access to the data center is restricted to qualified Memeo personnel only.

Memeo datacenters are equipped with redundant power from separate grids, redundant cooling systems, as well as multiple fiber links in and out of the facility. Diesel generators capable of running for an entire week back up the entire facility in case of catastrophic power loss.

All online backup data is stored on Amazon's S3 service. That means your precious files are stored in multiple datacenters, and in multiple states for redundancy to protect against natural disasters. Their protocols for storing data are safer and more secure than anyone else out there. No other storage provider can match the infrastructure that Amazon has built to host its storage platform.

Memeo also has emergency recovery plans in place which assure full recovery and operability within 72 hours in case of a major cata¬strophic event.

Facility

Memeo's server farm is hosted at an extremely hardened, state-of-the-art, secure data center in Nevada. The facility is built to the 'Tier 3 N+1' specification and features pre-action wet pipe and dry pipe fire suppression, triple-redundant power and cooling, as well as state of the art seismic bracing.

Key Features:

- Building Type – One story, non-load bearing tilt-up concrete construction with steel framing
- Fire Suppression – Double-interlocked, pre-action (dry pipe) + FM200 under floor; wet pipe backup
- Equipment and non-structural components, including cabinets, are anchored and braced.
- Liebert UPS. 125 kva, 15 minutes. Inspected quarterly. N+1 redundancy in all systems.
- Valve-Regulated Lead-Acid (VRLA) batteries providing a minimum of 15 minutes backup at full load.
- Automatic Transfer Switches (ATS) and bypass/isolation switches provide N+1 redundancy for dual source power capability.
- 24 x 7 national maintenance agreements for UPS and backup generator.
- Generator is sized to run entire site at full load for a minimum of 24 hours without refueling. Load tested weekly. Refuel agreement – guaranteed 4 hour response time.
- Full data-grade Liebert HVAC with redundant loop system (N+1 redundancy). 72° ambient air temperature (+/-2°), 45% humidity (+/-5%).Up-flow U302 cubic feet per second. Water detection system in bottom of cooling units

Physical Security

Memeo's data center utilizes an array of security equipment, techniques, and procedures to control, monitor, and record access to the facility. The site is monitored and recorded using CCTV, and all access points are controlled. There are 24-hour security officers to augment physical security features, providing financial-grade protection of our customer's mission-critical data. Employees are screened upon entry to verify identity and their access history is recorded.

Key Features:

- "Man Trap" Physical Entry
- 24x7 Security Guards
- CCTV surveillance and Video recorders
- Motion Detectors
- Biometric Hand Geometry Readers

Electronic Security

Memeo employees that require remote access to the Data Center are assigned a VPN account. VPN access allows connections to HTTP, HTTPS and SSH services running on Memeo's Control Server. It does not allow access to any other resource at the Data Center beyond these services.

If an employee requires shell access to servers at the Data Center other than the Control Server then they are assigned an individual SSH key. Again, a VPN account is required to connect to the Data Center so the key can be authenticated. All keys are authenticated and maintained by Memeo's Control Server. Employees must land on the Control Server before they are allowed to connect other resources.

If an employee resigns or is terminated by Memeo, Inc. then their VPN account is deleted from the NetOps Admin Server and their SSH key is deleted from the Control Server.

Network

Memeo's IP network intelligently routes customer traffic across major Internet backbones avoiding congestion and ensuring the fastest, most reliable data transfers possible.

Key Features:

- Full transit, route-control TCP/IP connectivity through our bandwidth provider direct to the major Internet backbones
- Proactive circuit monitoring and service troubleshooting 24/7 by Memeo's Network Operations Team
- Customer notification schedule and escalation procedures

Network Security

Memeo has a cluster of Juniper Secure Services Gateway Firewalls deployed at its network edge. Traffic flowing in and out of the data center is protected from worms, spyware, trojans, and malware by a complete set of security features that include stateful firewall, IPsec VPN, intrusion prevention system (IPS), anti-virus (includes antispyware, anti-adware, anti-phishing), anti-spam and Web filtering.

Data Integrity

Memeo takes the protection of our customer data very seriously. All customer data transferred to and from our service is protected by our secure data center infrastructure that has no single point of failure.

Key Features:

- High performance RAID 60 storage infrastructure that offers better data protection and capacity utilization than RAID 5 and RAID 1+0.
- 64-bit server architecture and the latest I/O technologies ensure the best file transfer performance
- Data snap-shot and snap-restore capability to ensure customer data availability and integrity

The Memeo Backup client communicates with Memeo servers over secure protocols to perform various tasks including:

- Login - For login authentication, OAUTH is used, an open protocol that allows secure API authorization. OAUTH is also used by leading web services companies such as Twitter, Flickr and Google.
- File upload and restore - As files are backed up and restored, a 128-bit SSL connection is established between the client and server. This ensures the connection is encrypted and secure.

- Access to Cloud Storage - Memeo uses Amazon S3's cloud storage infrastructure that utilizes a private key to access the data. This key can only be retrieved via our secure API using the Memeo Backup client.

Monitoring

Memeo utilizes several industry standard monitoring applications (Nagios, IPSentry, Munin and Cacti) to ensure that servers, switches, firewalls and load balancers are performing optimally in the data center environment. Operations personnel track CPU, memory, bandwidth, fan speed, temperature, load, I/O throughput, RAID controllers, individual drive temp, drive S.M.A.R.T status, and more. Frequency varies from 30 seconds to 5 minutes depending on the check.

About Memeo

Memeo Inc. is a Silicon Valley-based software and services company focused on providing data management services to small and medium businesses. Founded in 2003, Memeo provides easy-to-use backup, sync, and sharing solutions to simplify the protection and accessibility of valuable data. Memeo has 22 million customers and has shipped over shipped 65 million software licenses to more than 150 countries in 20 languages.