

System Security

System Security	Where applicable, MuseWorx uses a 1024bit or greater encryption.
Data Security	All data is physically and electronically secured in one of our multiple data temperature controlled centers.
Configuration	Systems operates on a Windows Server Platform, utilizing Microsoft SQL for its data structure.
Capacity	Data Storage is equivalent to multiple Petra bytes or as required.
Redundancy	Our backbone connection to the Internet is “multi-homed” and employs direct optical links to the major Internet backbones. Our primary Data Center is located in San Diego Tech Center campus – a meeting point for 10 major carriers including MCI, Level3, AT&T, Time Warner, SBC, XO Communications, and Williams.
Scalability	All equipment is scalable automatically for data, storage and servers.
Technical Support	Emphasis on the quality of customer support. We offer live customer support. In addition, we actively maintain an interactive Knowledge Base which currently contains over 2,500 support documents.
Other	MuseWorx takes pride in maintaining a 99.9% up time

System Security

SAS 70 TYP-II Certified Data Center

Third-party SAS 70 certification ensures the data center implements the necessary controls to enforce security.



Cisco PIX Firewall

Professionally managed CISCO firewalls protect every server.

Physical access control

Physical access to systems containing confidential files is controlled and monitored. The service is housed in state-of-the-art data centers featuring 24x7 guarded access facilities using a wide range of security systems including video camera surveillance and the latest in iris and palm scanning technologies.

Network access control

Network access to systems is highly restricted. The service utilizes firewalls to shield servers from the Internet and restricting access to only HTTP ports. This denies any network-based access to systems that may compromise security.

Encrypted transmission

Data transmissions over any network are always encrypted for upgraded accounts. Files are uploaded and downloaded from the service using SSL encryption

Internal user authentication

Each internal user is assigned a unique ID and password for authentication. Passwords are required to be least 6 characters to ensure integrity. Stronger passwords can be set at the user's discretion. In addition, passwords are encrypted to ensure integrity.

External user authentication

To collaborate or download a file, the receiver must first have their own assigned username and password (if the user has not selected "Public Share"). To prevent unauthorized access the receiver must provide the username and password matched to the receiver's email address.

Authorization system

The authorization system works in conjunction with authentication and protection to enforce granular access to information. Each user must authenticate to start a session every time they use the service. The session carries user credentials that are compared against permissions for every request. This enables the service to enforce permissions at the application level for restricting access to authenticated users only.