mimeo

SECURITY

DIGITAL & PHYSICAL

Digital Security

Encrypted Document Transfer

Each time a file is uploaded to Mimeo, a unique certificate is automatically assigned to the user. The file can only be decrypted by Mimeo during the transfer of this data. A secure protocol (HTTPS) and Secure Sockets Layer (SSL) is utilized within all of Mimeo's platforms. These are the same encrypted document transfer technologies utilized by financial and retail institutions. Numerous financial services companies in the Fortune 100 entrust Mimeo to secure their content.

Data Encryption

Data is encrypted during every step of its journey, including while the data is in flight and at rest. While at rest, the data is AES 256 FIPS 140-2 Level 2 Compliant. At Transfer, SSL Class 3 EV SHA256.

Most of the Fortune 100 Financial Services companies entrust Mimeo to secure and distribute their printed and digital content.

Critical Data Safeguards

Mimeo ensures that critical data safeguards are fully implemented throughout our organization. Critical data, address book files and documents all have restricted access. All PII (Personally Identifiable Information) of our customers remains fully protected, and will not be sold, leased, or shared with any other companies, except those who need it to help us serve you (e.g. providing your name, and address to our third party shipping agent and payment processor -with whom we share your financial information to fulfill payment). ***Additionally, Mimeo offers a fully PCI compliant payment option.***

IT Security

Mimeo server networks are separated behind redundant firewalls. Access control lists and event logs are regularly monitored and reviewed, preventing unauthorized activity. All customer data is protected by these industry leading firewalls.

3-Tier Architecture

Need-to-Know Basis

Need-to-know basis is a discipline implemented across Mimeo globally. It prohibits all unnecessary access by employees to information and areas that are not relevant to their roles and responsibilities. Access to customer data is limited by machine, network, user, location, and application. Infrastructure event logs are regularly reviewed to monitor access and provide audit trails.

File Deletion

Our customers own all of their data, all of the time. Mimeo users have the ability to delete any of their files and documents associated with Mimeo at anytime. When a user deletes a file from their account, the file is removed internally from our systems and permanently deleted.

TRUSTe Certified

TRUSTe is the leading global Digital Privacy Management (DPM) company. Mimeo.com has earned this widely recognized TRUSTe certificate through the protection of its customers personal account information. To maintain this certification, audits are held on an annual basis.

Password-Protected Accounts

An account created through any of Mimeo's platforms requires a fully customizable password for access. Customers set and control their own passwords, and Mimeo employees do not have access to them. In the event of a password being lost, customer care representatives can utilize an automated system that resets the password, prompting the user to immediately change it.

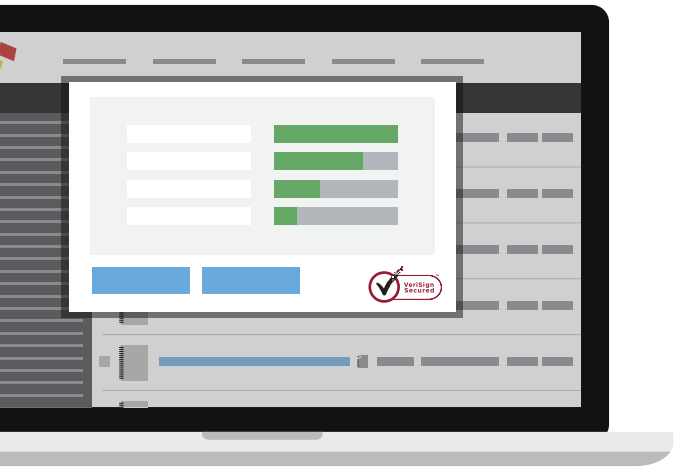
Additionally, Mimeo offers Single sign-on (SSO), designed for use within a private Mimeo Marketplace. SSO is a method of access control that enables users to initially authenticate their login credentials. The account can then be directly accessed without entering login credentials. Our customers utilize SSOs through their corporate intranet, LMS system, or any other system that is deemed to be a trusted authority.

Risk Management

Mimeo performs internal risk assessment, including physical inspections, access audits, software audits, and external pen tests.

Print Driver

Mimeo allows customers to 'Just Hit Print' through the use of the Mimeo Print Driver. This internet file transfer manager allows Mimeo to appear as a printer option on your computer, radically improving the upload experience. The same encryption level is utilized for the Mimeo Print Driver as for individual accounts and SSO. Additional information, including installation, can be on our website at http://www.mimeo.com/support/mimeo-printer



Upload Manager

Mimeo compresses and encrypts all content that is uploaded to our platform. Secure Socket Layer (SSL) and HTTPS technology are utilized through all data transfers. including all traffic to and from Mimeo. Through SSL, Mimeo is VeriSign Secured.

Browser Support

Mimeo supports the most recent versions of Google Chrome, Firefox, Safari, and Internet Explorer.

AV Protection

Antivirus programs are in place organization wide to prevent infections caused by many types of malware, including worms, Trojan horses, rootkits, spyware, keyloggers, ransomware and adware.

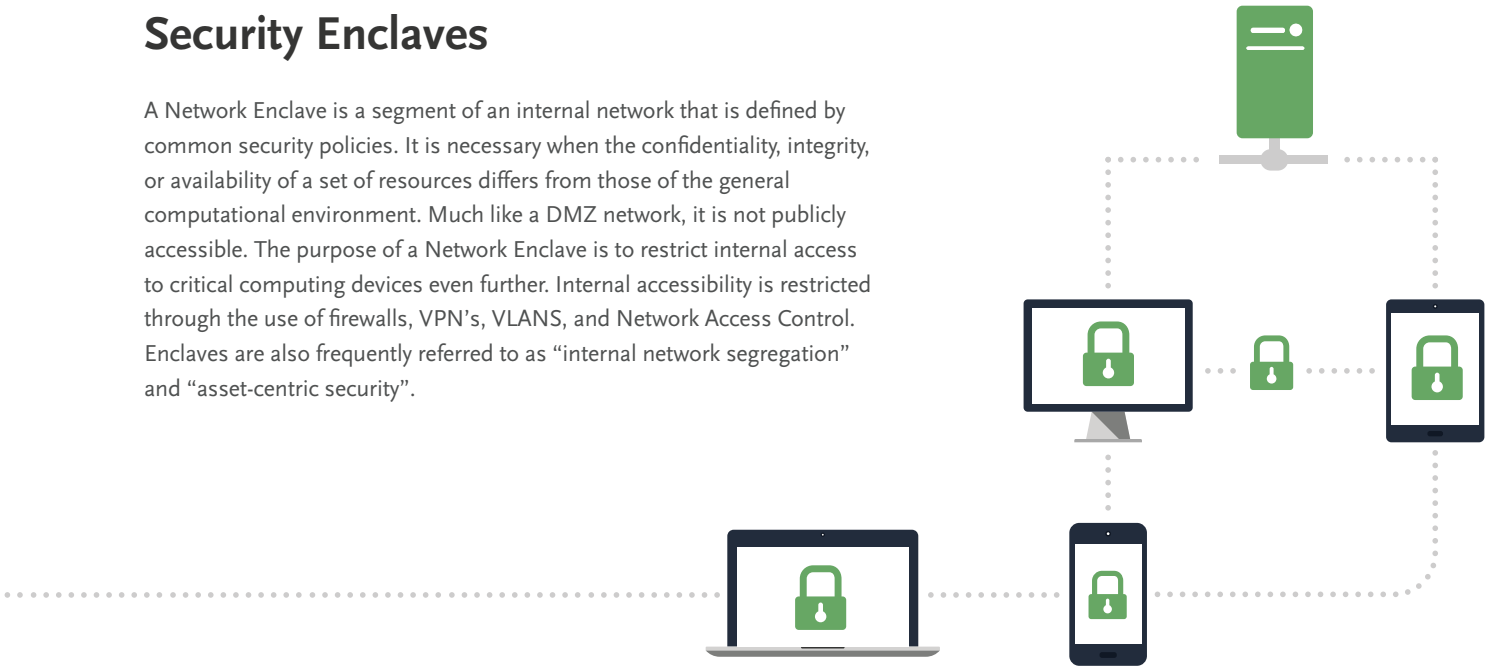
Endpoint Security

Each device with a remote connecting to the network creates a potential entry point for security threats. Mimeo fully implements endpoint security, a methodology of protecting our corporate network when accessed via remote devices such as laptops or other wireless and mobile devices.

Endpoint security management is a policy-based approach to network security that requires endpoint devices to comply with specific criteria before they are granted access to network resources. Endpoints can include PCs, laptops, smart phones, tablets and specialized equipment such as barcode readers or point of sale (POS) terminals.

Security Enclaves

A Network Enclave is a segment of an internal network that is defined by common security policies. It is necessary when the confidentiality, integrity, or availability of a set of resources differs from those of the general computational environment. Much like a DMZ network, it is not publicly accessible. The purpose of a Network Enclave is to restrict internal access to critical computing devices even further. Internal accessibility is restricted through the use of firewalls, VPN's, VLANS, and Network Access Control. Enclaves are also frequently referred to as "internal network segregation" and "asset-centric security".



Physical Security

Facility Access Control

Employees are granted access only to those tools required to complete the tasks assigned to them. The Mimeo production process is managed by sophisticated, computerized systems that govern all access control and task allocation to fully prevent any unnecessary access.

Additionally, RFID card access has been implemented across all of our global facilities.

Facility Security

Through the dedication of our facility teams and multiple layers of security, Mimeo has implemented a unified security program at each of its global production facilities. Employees are monitored and recorded using secure surveillance equipment. Magnetic key cards limit movement within designated areas of the facility. These additional measures have been implemented:

- A perimeter fence surrounds production facilities.
- 24/7 recorded video surveillance is implemented through tilt and zoom cameras. These cameras cover all key areas. Footage is reviewed regularly.
- A state-of-the-art alarm system from an elite security company includes motion detectors and an audible alarm. Only select employees are privy to the alarm codes. Each group is assigned a different alarm code to enable regular updating, as well as immediate change in the event of turnover.
- A card-reader security system allows employees and visitors access only to specific, authorized areas while tracking movement through all locked doors.
- Different color security badges, which must be worn and displayed at all times, differentiate employees from visitors. Certain badges require that a Mimeo employee accompanies the visitor at all times.
- All employees of the facility are empowered to stop anyone they do not recognize to request credentials and authorization.
- Personal Cameras and cell phones are prohibited on the production floor.
- No personal handbags, purses or backpacks are allowed on our production floors.
- No loose jackets are allowed to be worn within the parameters of our production facilities.
- Fire suppression systems are installed within our production facilities.
- Guards patrol all production facilities.

Uninterruptable Power Supply (UPS)

In the event of power failure caused by outages or inclement weather, Mimeo's production facilities automatically utilize an uninterruptable power supply (UPS), ensuring continuous operation and full security implementation. Mimeo utilizes UPS that operates for 3 consecutive days without refueling. Additionally, contracts are in place that guarantee Mimeo priority during extended crisis events. We pride ourselves in being available for our customers 24 hours a day, 7 days a week, with no downtime.

Redundant Data Centers

All customer data is stored on Mimeo owned, redundant, fully protected data centers in two locations. All cloud based terminology refers to Mimeo's own internal cloud. None of our customer data is hosted on third party servers.

Employee Trust

All Mimeo employees are subject to extensive background checks prior to employment. Mimeo employees sign a legally binding confidentiality agreement that governs their conduct. Employees are held personally responsible for any unauthorized use of the information entrusted to Mimeo.

Mimeo employees complete annual and periodic confidentiality and security awareness training.

Supplier Qualification

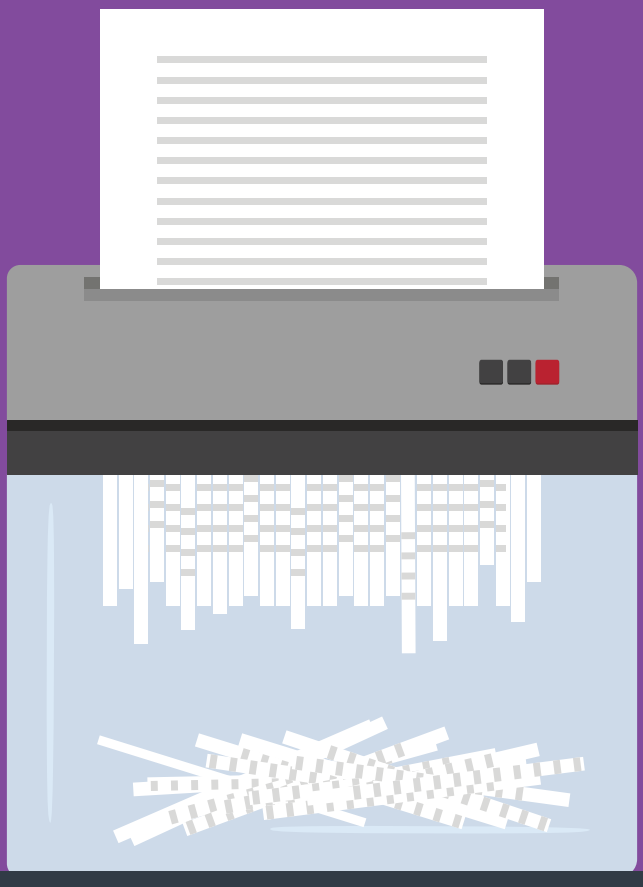
We hold all of our suppliers to the highest standards. Some of the qualifying standards we set during supplier assessment include:

Document Security

All documents are stretch film banded during production, preventing any tampering, and ensuring that 100% of each ordered document is delivered to our customers.

Document Disposal

Any document created during the production process that is not shipped to a customer as part of an order is immediately shredded. Documents requested by a customer to be destroyed are placed in locked, metal bins both prior to and after being destroyed.




mimeo