

World Class Security

Security Technology, Processes and Procedures



0808.208.4260 (Int'l +1.901.566.5509)
mimeo.co.uk


mimeo.co.uk™



Mimeo.co.uk sets a new standard for document security.

Mimeo.co.uk's industry-leading processes and procedures ensure the highest level of confidentiality and safety for your data throughout the order and fulfillment process. Mimeo has carefully created its processes with unique security measures that no other supplier – external or internal – can replicate.

Digital Files and File Transmissions

- **Encrypted Document Transfer:**
When a print file is transmitted to the Mimeo web site, the user will automatically receive a unique certificate, encrypting data in a format that can only be decrypted by Mimeo. This technology is commonly known as Secure Sockets Layer (SSL or HTTPS), and it is the same technology used by financial and retail institutions to conduct secure e-commerce over the Internet.
- **Access Security:**
The Mimeo production process is managed by sophisticated, computerised systems that govern all tasks, including access control. Individual Mimeo employees are granted access only to those tools required to complete the tasks assigned to them.
- **Critical Data Safeguards:**
The same computerised system restricts access to critical data, including credit card information, address book files and document files.

- **Password-Protected Accounts:**

Individual Mimeo accounts are password-encrypted to prohibit unauthorised access to the contents of an account holder's documents, files and address information. Customers set and control their own passwords.

- **File Deletion:**

Customers may select files and documents from their digital library to delete at any time.

- **Confidentiality Agreement:**

All Mimeo employees sign a binding confidentiality agreement that governs their conduct. Employees are held personally responsible for any unauthorised use of the information entrusted to Mimeo.

- **TrustE Certified:**

The Mimeo site has earned the widely recognised TrustE certificate, indicating that we recognise and protect the privacy of all personal information collected in our customers' accounts.



Physical Security

- **Security System:**

Our centralised production facility is protected by a state-of-the-art security system. All areas of the facility are monitored and recorded using secure surveillance equipment. Magnetic key cards limit movement within designated areas of the facility and throughout the building.

- **Document Security:**

Each document is shrink-wrapped during production, protecting the confidentiality of all content, preventing any tampering, and ensuring that the recipient receives 100% of the ordered document.

- **Document Disposal:**

Any document created during the production process that is not shipped to a customer as part of an order is securely disposed of the same day.

“ *Nothing leaves the Mimeo facility that isn't shrink-wrapped or destroyed.* ”

— Andy Nied, VP, Worldwide Production

Security Technology Overview

Mimeo is the leading provider of technology-enabled, outsourced print solutions for professionals and corporations. Shifting the traditional print paradigm to incorporate the Internet, our solution involves the installation of a print driver – a surrogate for the actual printer we will use to create our customer’s documents – and an Internet file transfer manager on the customer’s desktop that lets customers print from any Windows-based application. Customers simply select “Print” from the application’s drop-down menu and select the “Mimeo.co.uk Printer.”

Our Mimeo Printer software consists of two primary software components. The first is a traditional print driver and associated port monitor. Installation may require access rights beyond those granted to typical users (see Note below).

Note: In some versions of Microsoft Operating Systems, installing a print driver requires administrative rights above those typically assigned to users. For that reason, depending on the site policy, administrators may have to install the Mimeo Printer software for those users who have insufficient access rights. Once the Mimeo Printer software is installed, anyone can use the service, regardless of that user’s assigned level of access.



The second component, called the Upload Manager, compresses and uploads print files to the Mimeo Web site. All print files are sent as compressed, print-driver generated PostScript files over the Secure Socket Layer (SSL) protocol, which is the same protocol that is used by all institutions for conducting secure financial transactions over the Internet. With the exception of a dependency on Microsoft’s “Winlnet.dll,” the entire Upload Manager is a lightweight process with no system interactions or special requirements. (The first phase, or upload phase of the process, has a dependency on Microsoft’s Internet Explorer as described in the section entitled “Internet Upload and Mimeo Dependencies.”)

The cornerstone of our Mimeo Printer software is an industry standard PostScript print driver. The PostScript driver ensures that all file data is translated correctly to printer-formatted output before it is transferred from the user’s workstation.

Without the Mimeo Printer, print files transferred from a workstation as a complex application document (i.e., Word, PowerPoint, etc.) can “drop” important data elements, such as fonts, linked graphics and margin settings. Using the Mimeo Printer alleviates the traditional challenge of files “leaving behind” valuable pieces of information. It ensures that what the user sees on their monitor is an exact representation of the final output.

Web-Based Document Configuration

The first phase of document creation requires uploading a print file into the Mimeo library using the Upload Manager. After a file is added to the library, Mimeo launches the user's default Web browser to continue the second phase of document creation – document configuration. Document configuration allows the user to select options, such as colour vs. black & white printing, single- or double-sided printing, paper selection, cover selection, binding options, tab configuration and mailing destinations. This process works with the user's browser over a Secure Socket Layer (SSL) connection. Both upload and configuration steps require SSL access to Mimeo web servers.



Internet Upload and Mimeo.co.uk Dependencies

Mimeo upload software depends on “Wininet.dll.” If users have a fully-configured version of Microsoft Internet Explorer (6.0+), they should have no difficulty navigating within their corporate Intranet when uploading to the Mimeo server.

In order for Mimeo's client-based Upload Manager to transmit the customer's print file to Mimeo.co.uk, it must be able to find our upload servers and establish a connection to our upload server software. Since virtually every corporation uses proxy servers and/or firewalls to connect their workstations to the Internet, various configurations of firewalls and proxy servers will lie between our client's workstation and our upload servers. Our client software will have to negotiate a pathway through these devices as it finds and connects to our upload servers. Proper connectivity setup can usually be determined by simply using Internet Explorer

to connect to any HTTP and HTTPS site. By connecting to the Mimeo.co.uk Web site (HTTP), establishing an account, and logging into your account (HTTPS), you will have established that IE is properly configured.

The information contained on this page is intended for persons responsible for the support of Windows workstations and those knowledgeable in the configuration of Microsoft's Internet Explorer for the local network environment.



Workstation Access Rights

In order to generate the print format used by Mimeo printers, an industry standard PostScript print driver is installed onto the user's workstation, which, as is the case with any Windows print driver, may require advanced access rights on some workstations.



Firewalls and Proxy Servers

There is no need to open special ports or enable special applications on any of the user's firewalls or proxy servers to accommodate the Mimeo print service; we upload print data securely using the same standard HTTPS protocols (port 443) used for all secure online transactions. Because Mimeo manages the printer configuration at a central facility, there is no need to install the print driver on a shared server for ease of administration; the driver is only being used to generate PostScript and requires no supervision or administration on the part of the user's infrastructure support personnel.

Mimeo.co.uk has three web sites with which users interact. The first web site is simply our external or public web site, accessible via HTTP by anyone with an Internet connection. The second two are customer-specific web sites, accessed only via SSL or HTTPS protocols. For this reason, users require the ability to connect over SSL to Mimeo's upload servers as well as to the user's individual library.



Frequently Asked Questions



Does Mimeo have an information security program in place (e.g. policies, procedures, security awareness, incident response, a designated security officer)?

1 We leverage industry standard network and physical security hardware and systems to keep internal and customer data secure from unauthorised access. In addition to employing a well-defined set of security policies, procedures, education and best practices to monitor and enforce these measures, we have successfully passed security audits from our corporate customers, including those conducted by some of the most recognised names in the financial services, pharmaceutical, and technology industries. Annual audits by TrustE additionally confirm our privacy policy compliance.

What type of access controls are used for Mimeo's service or application (e.g. approval process, separation of duties, removal from access, application/system/network protection)?

2 Access control to business data is managed through network and software permission controls, while specific network resources and infrastructure access are managed via user and group permissions. Server networks are separated behind redundant firewalls. Access control lists and event logs are monitored and reviewed to prevent unauthorised access from machines on the network. Industry standard firewalls protect Mimeo customer data from outside access, while in-house resources monitor firewall activity, implementing appropriate policies to ensure protection and controls. Mimeo's technology securely connects our facilities, allows for secure data transfer, monitoring and protection from unauthorised use.

The MIS team exclusively controls the creation and use of infrastructure passwords. Access to customer data is limited by machine, network, user and application. Customer data is only made available on a need-to-know basis, and infrastructure event logs are reviewed to monitor access and provide audit trails. Customer print data is controlled through the infrastructure configuration and not directly handled by print production personnel. Our print production systems securely route print data directly to presses in the production facility, and, for added firewall security, monitoring alerts the MIS team to any firewall abnormality.

What policies, standards, and procedures are in place for identification and authentication?

3

Individual customers manage their own usernames (email address) and passwords. The password policy requires a minimum of 7 characters, including at least one numeric or special character. Users associated with a corporate customer account cannot change their usernames but are responsible for managing their own passwords.

All password-protected communication with the customer through the Mimeo.co.uk Web site is secured via SSL encryption, including the uploading of print file data (email and ftp are not used).

The Mimeo network uses NTLM. All users sign on to the company network with usernames and passwords. In addition, remote users require a different ID and Password to connect to the network VPN via 3DES security algorithms.

How is anti-virus or other anti-malicious code software configured and managed for maximum effectiveness throughout the servicing organisation?

4

Mimeo employs a virus protection service on its email servers to protect all incoming and outgoing email from viruses.

All print file data uploaded by customers is translated from the native application format to PostScript by the Mimeo print driver and upload manager applications securing the transfer from potential viruses.

All Mimeo PC's and systems run with virus protection software. All systems check for updated virus definitions hourly.

How is Mimeo's change control process performed for product development, test and production?

5

Mimeo.co.uk development incorporates Microsoft Team System and the Agile methodology. The product release process applies the appropriate controls and assurances – for example, a release database, a release day task checklist, a bug capture system for testing cycles and SWAT meeting(s) prior to a release.

How is my information protected from unauthorised access or disclosure during transit and while in storage from origination to destination (e.g. firewalls, virtual private networks, intrusion detection, encryption)?

6

Industry standard firewalls protect customer data from unauthorised access. In-house resources monitor firewall activity while implementing appropriate policies to ensure protection and controls. All communication of customer data is secured via SSL encryption. Network-based intrusion prevention and host-based intrusion detection systems monitor network and systems activities.

What physical security provisions are in place to ensure information, systems, and operations are adequately protected?

7

A specialist in the protection of classified security assets and our current independent security consultant contributed to the design and implementation of a physical security plan for our 13,000 m², highly automated digital print facility.

- A perimeter fence surrounds the facility.
- 24/7 recorded video surveillance through tilt and zoom camera covers all key areas and is reviewed periodically.
- 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, and each group is assigned a different code so that codes can be updated and changed in the event of turnover.
- A card-reader security system allows employees and visitors access only to specific, authorised areas while tracking movement through all locked doors.
- Different colour 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 recognise to request credentials and authorisation.
- All printed materials that leave the facility are either shrink-wrapped and securely packed and sealed for delivery or shredded within two hours of printing and sent to be recycled on a weekly basis.

How is the integrity (assurance of accuracy) of my customer information protected?

8

All print file data transmitted from the customer via the Mimeo print driver and upload manager is encoded to ensure accuracy. Customers also benefit from real-time electronic soft-copy proofs of their documents to verify accuracy before ordering.

How is my information protected from loss or disclosure due to system failure and disasters?

9

All customer data is fully protected on real-time, redundant data storage devices in data centres in two physical locations. As an added precaution, all data is backed up in both locations. Customer data is destroyed upon customer's request.

What audit logs are maintained for user activities and system/application processes? How are they monitored, protected online, and stored long-term offline?

10

Audit logs are maintained over a period of at least one year, depending on the type and verbosity of the captured data. Application login access is logged on a per user basis. Web logs capture application usage, errors and security violations. Print production process logs capture all production floor print job access and status changes by operator. Windows security logs capture internal system access and security violations. Firewall, VPN, email and virus protection system logs are captured and actively monitored by systems and Data Security staff.



Print and Ship with a Click

UK: 0808.208.4260

International: +1.901.566.5509

US: 1.800.GoMimeo (1.800.466.4636)