

MetroFax® Privacy Information

Is your fax machine keeping a dirty little secret? Some fax machines use a film cartridge for the toner used to print your incoming faxes. That film is like a photo negative of every fax you receive. If someone were to obtain that film, they can see every fax you've received.

Even high tech faxing equipment isn't always secure. Some fax machines or all-in-one devices use hard drives to temporarily save faxes that are sent or received. These hard drives are usually not encrypted and many times end up discarded or even resold without the information being securely erased.

What happens to a paper fax? Unfortunately, in businesses or in home offices, faxes end up in the recycling bin. How secure is your recycling bin? A fax with personal identity or confidential information can easily be obtained by dumpster divers.

Would you leave your paystub lying on a table in the copy room? Of course not. However, in many offices, a fax machine is a treasure trove of information in a non-secure location where anyone with access can read or take paper faxes printed or sent from the fax machine. Securing paper documents is difficult in most situations.

Practicing good privacy policies is no longer optional, it's the law. Many companies are now faced with compliance with HIPAA and other regulations regarding personal information. The disclosure of confidential or personal information can subject your organization to fines, civil penalties, and embarrassing public relations.

When sending or receiving faxes, you don't want to worry about information getting into the wrong hands.

- ▶ Identity Theft
- ▶ Financial Statements and Records
- ▶ Disclosure of Confidential Information

MetroFax Helps Protect Against Fax Privacy and Security Breaches

MetroFax enables you to eliminate the "paper trail" of traditional faxing.

DIRECT TO AND FROM YOUR EMAIL ACCOUNT

Faxes are securely sent to and from your computer to the MetroFax service with the latest SSL encryption technology. This is the same technology that helps to protect the privacy of your banking and other online transactions.

DIRECT TO AND FROM THE METROFAX DASHBOARD

With the MetroFax Dashboard your faxes are securely processed, sent, and received on the MetroFax servers. Each user must have a valid username and password, which is SSL-encrypted for your protection.

Whether you're a one-person office or a large organization, each person can have his or her own fax account. Faxes go directly to each person's account keeping prying eyes from faxes.

For extra security, send and receive faxes directly on the MetroFax service with our exclusive MetroFax Dashboard.

METROFAX TAKES SECURITY AND PRIVACY SERIOUSLY. WE HAVE THE FOLLOWING SAFEGUARDS IN PLACE TO PROTECT YOUR DATA:

Data Encryption

MetroFax uses Secure Sockets Layer (SSL) technology. MetroFax uses the strongest commercially available encryption products including 128-bit VeriSign SSL Certification and 2048-bit RSA public keys. MetroFax also supports Transport Layer Security (TLS) as an added encryption technology to help send secure information over the public Internet from your computer to the MetroFax servers. For increased security, dedicated point-to-point virtual private network (VPN) solutions are also available.

Application Security

When you send a fax with MetroFax from your existing email account, that email client's access controls are used, including your username and password. When you use the MetroFax Fax Printer or use your Web browser to connect the MetroFax Dashboard all accounts must use a unique user identification, such as a username and password.

Operating System Security

MetroFax maintains tight control of our service infrastructure and does not outsource the operation or maintenance of our production servers. A limited number of MetroFax personnel have access to production servers. In addition to regular security reviews of server logs and processes, we deploy software monitoring for attempted security breaches of our systems. To reduce potential security threats, we disable any service, protocol, user/group access accounts, and applications that are not required for the operation or maintenance of our systems.

Physical Safeguards

The MetroFax data center includes state-of-the-art redundant electrical power, cooling, and telecommunication facilities. Our data center is a multi-layered secure facility that includes 24x7x365 manned security and checkpoints, closed circuit television (CCTV) cameras with continuous video recording of all entrances,

exits, and data rooms. All egress and ingress activity into the MetroFax data center is restricted to a limited number of approved personnel and is recorded.

Internal Systems Security

MetroFax diligently protects the integrity of our internal network, including all hardware and software. In addition, we use leading third-party antivirus software that is frequently updated automatically to prevent the introduction of malicious code into our network infrastructure.

Server Management Security

Customer data, including faxes sent, received, and saved on MetroFax services is protected and secure. Data is only accessible by the account holder and authorized personnel for the purposes of system maintenance, monitoring, or compliance with legal or court orders. Faxes and their contents are the property and liability of the account holder. Customer data is saved on secure systems that are behind firewalls with active intrusion monitoring and countermeasures. MetroFax does not outsource the operation or maintenance of our production servers.

Reliability and Backup

Industry standard practices are followed for data provider redundancies, load balancing, and equipment failover scenarios.

MetroFax utilizes physical measures, policies, and procedures to protect electronic information systems, facilities, equipment from natural and environmental hazards including unauthorized intrusion. The MetroFax data center includes state-of-the-art redundant electrical power, cooling, and telecommunication facilities. Customer data is maintained on geographically dispersed redundant disk-based storage to prevent catastrophic data storage failure. MetroFax has a disaster recovery plan in the unlikely event of an interruption to our primary services.