

Data Transfer Policy:

All sensitive data transmitted to Reflections printing will be done so through Secure FTP (Secure File Transfer Protocol). Secure FTP (SFTP) has become the preferred file transfer method for companies that need to transfer electronic documents over the Internet. SFTP is specifically designed to handle large files and sensitive data. Using Secure Sockets Layer (SSL) technology, the standard in Internet security, SFTP ensures unreadable data transmissions over the Internet even without a proper digital certificate. Its confidential data transfer protection is the primary benefit of SFTP.

Data Storage Policy:

Theft or loss of corporate intellectual property is an increasing concern for organizations. Reflection's utilizes Drive Encryption technology. This technology provides full file or folder encryption, which helps protect data from being compromised on a lost or stolen machine.

About the Reflections Printing Network:

The following is a summary of security practices and precautions used at all times by Reflections Printing.

- We utilize a Stateful Packet Inspection Firewall.
- Have a valid Network AntiVirus subscription.
- Automated Anti-Spyware software on all computers.
- SPAM filtering.
- Complex Password Policy with periodic forced changes.
- Off Site Backup using password protected media.
- Servers in a locked room with limited access. All servers have locking screen savers.
- Critical Microsoft patches automatically installed.
- Office security system and state of the art surveillance system.

Reflections Printing takes data security very seriously and follows thorough procedures for maintaining the integrity of our customers' data perimeter.