ECSI Security

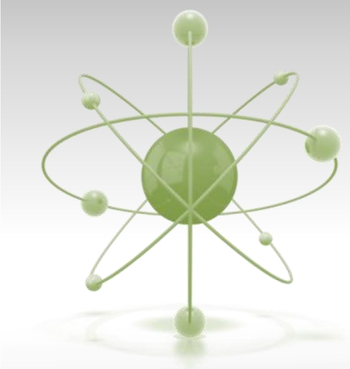
Secure Data Transfer Methods

ECSI's Commitment to Security

The security and protection of your confidential information is extremely important to us. ECSI supports several methods for you to send this confidential information securely. Our FCRYPT solution was available years before "Identify Theft" or the myriad of data-loss stories became almost daily headlines in your local newspaper. Where the accepted standard for bank-to-bank exchange of information is 256-bits, ECSI provides a 448-bit solution which is exponentially more secure (commonly called military-grade).

We suggest that you take full advantage of one of the following methods and we STRONGLY suggest that you NEVER send confidential information in the body of an email, as an unencrypted email attachment (e.g., a spreadsheet), or in any plain text using open FTP (File Transfer Protocol).

1. FCRYPT: FCRYPT is a stand-alone encryption program that ECSI has provided since 1999. It is based on Blowfish and a client-specific, 448-bit key. It is extremely secure and very easy to use. Files encrypted with FCRYPT can be sent safely via email, open FTP, or any other electronic method with complete confidence.
2. PGP: ECSI added PGP (Pretty Good Privacy) as an option in 2002. PGP uses a public/private key scheme. Setup is a bit more involved but can be accomplished by most users. Files encrypted with PGP can be sent safely via email, open FTP, or any other electronic method with confidence.
3. WinZip Encrypted Zip Files: Since the release of WinZip version 9, ECSI has accepted password protected, encrypted zip files. WinZip 10 (the current version) supports 128-bit and 256-bit AES encryption, which are very secure. WinZip files encrypted with AES can be sent safely.
4. Secure FTP: sFTP allows you to send files (encrypted or not) securely from your machine to our server. ECSI made our sFTP server available in 2005. The largest advantage of sFTP is to prevent someone from intercepting your FTP login ID, password, or the confidential data sent between you and ECSI. ECSI will provide a free sFTP client upon request. For maximum safety, we suggest you encrypt the file with FCRYPT prior to sending with sFTP.
5. Secure Forms: Introduced in 2006, Secure Forms allow you to provide common information securely over our web site (e.g., exit requests, advance requests, etc). Instead of putting this information into an unsecure email, you provide the relevant data on a web form. The request is formatted and submitted securely to our customer service department for processing.
6. Secure Messages: Also introduced in 2006, Secure Messages allow you to make free-form requests to any of the main departments at ECSI. Secure Messages are a good replacement for sending unsecure email to ECSI and are just as easy as your email program. You can include SSNs, demographics, dollars, etc. with complete confidence.



Unfortunately, by its very nature, the subject of encryption can be a complicated discussion. If any of this sounds like 'geek-speak', please forward this document to a member of your IT staff or feel free to contact ECSI for further assistance.

Please feel free to contact us at 1-800-437-6931 or email us at clientsupport@ecsi.net and we'd be glad to assist you.